
A BILL FOR AN ACT

RELATING TO THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

1 SECTION 1. The Hawaii Revised Statutes is amended by
2 adding a new chapter to be appropriately designated and to read
3 as follows:

4 "CHAPTER

5 THE UNIFORM EMPLOYEE AND STUDENT ONLINE PRIVACY PROTECTION ACT

6 § -1 Short title. This chapter may be cited as the
7 uniform employee and student online privacy protection act.

8 § -2 Definitions. As used in this chapter:

9 "Applicant" means an applicant for employment.

10 "Educational institution" means:

- 11 (1) A private or public school, institution, or school
- 12 district, or any subdivision thereof, that offers
- 13 participants, students, or trainees an organized
- 14 course of study or training that is academic, trade-
- 15 oriented, or preparatory for gainful employment;



- 1 (2) School employees and agents acting under the authority
- 2 or on behalf of an educational institution; and
- 3 (3) Any state or local educational agency authorized to
- 4 direct or control an entity described in paragraph (1)
- 5 of this definition.

6 "Electronic" means relating to technology having

7 electrical, digital, magnetic, wireless, optical,

8 electromagnetic, or similar capabilities.

9 "Employee" means an individual who provides services or

10 labor to an employer in exchange for salary, wages, or other

11 remuneration or compensation.

12 "Employer" means a person that provides salary, wages, or

13 the equivalent to an employee in exchange for services or labor.

14 The term includes an agent or designee of the employer acting

15 under the authority or on behalf of an employer.

16 "Personal online account" means any online account

17 maintained by an employee or student, including social media or

18 electronic mail accounts, that is protected by a login

19 requirement. The term does not include an account, or the

20 discrete portion of an account, that was:

- 21 (1) Opened at an employer's behest, or provided by an
- 22 employer and intended to be used solely or primarily



1 on behalf of or under the direction of the employer;
2 or

3 (2) Opened at an educational institution's behest, or
4 provided by an educational institution and intended to
5 be used solely or primarily on behalf of or under the
6 direction of the educational institution.

7 "Prospective student" means an applicant for admission to
8 an educational institution.

9 "Publicly available" means available to the general public.

10 "Specifically identified content" means data or information
11 on a personal online account that is identified with sufficient
12 particularity to:

13 (1) Demonstrate prior knowledge of the content's details;
14 and

15 (2) Distinguish the content from other data or information
16 on the account with which it may share similar
17 characteristics.

18 "Student" means any full-time or part-time student,
19 participant, or trainee who is enrolled in a class or any other
20 organized course of study at an educational institution.



1 § -3 Protection of employee or applicant online account.

2 (a) Subject to the exceptions in subsection (b), an employer
3 shall not:

4 (1) Require, coerce, or request an employee or applicant
5 to:

6 (A) Disclose the user name and password, password, or
7 any other means of authentication, or to provide
8 access through the user name or password, to a
9 personal online account;

10 (B) Disclose the non-public content of a personal
11 online account;

12 (C) Provide password or authentication information to
13 a personal technological device for the purpose
14 of gaining access to a personal online account,
15 or turn over an unlocked personal technological
16 device for the purpose of gaining access to a
17 personal online account;

18 (D) Alter the settings of the personal online account
19 in a manner that makes the content of the
20 personal online account more accessible to
21 others; or



1 (E) Access the personal online account in the
2 presence of the employer in a manner that enables
3 the employer to observe the content of the
4 account;

5 (2) Require or coerce an employee or applicant to add
6 anyone, including the employer, to the employee's or
7 applicant's list of contacts associated with a
8 personal online account;

9 (3) Take, or threaten to take, adverse action against an
10 employee or applicant for failure to comply with an
11 employer requirement, coercive action, or request that
12 violates paragraph (1); or

13 (4) Fail or refuse to admit any applicant as a result of
14 the applicant's refusal to disclose any information or
15 take any action specified in paragraph (1).

16 (b) Nothing in subsection (a) shall prevent an employer
17 from:

18 (1) Accessing information about an employee or applicant
19 that is publicly available;

20 (2) Complying with a federal or state law, court order, or
21 rule of a self-regulatory organization established by
22 federal or state statute, including a self-regulatory



1 organization as defined in section 3(a)(26) of the
2 Securities Exchange Act of 1934 (15 U.S.C.
3 78c(a)(26));

4 (3) Without requesting or requiring an employee or
5 applicant to provide a user name and password,
6 password, or other means of authentication that
7 provides access to a personal online account,
8 requiring or requesting an employee or applicant to
9 provide specifically identified content that has been
10 reported to the employer for the purpose of:

11 (A) Enabling the employer to comply with legal and
12 regulatory obligations;

13 (B) Investigating an allegation, based on the receipt
14 of information regarding specifically identified
15 content, of the unauthorized transfer of an
16 employer's proprietary or confidential
17 information or financial data to an employee's or
18 applicant's personal online account;

19 (C) Investigating an allegation, based on the receipt
20 of information regarding specifically identified
21 content, of unlawful harassment or threats of
22 violence in the workplace; or



- 1 (D) Protecting against a threat to safety, employer
2 information technology, communications technology
3 systems, or employer property;
- 4 (4) Prohibiting an employee or applicant from using a
5 personal online account for business purposes; or
- 6 (5) Prohibiting an employee or applicant from accessing or
7 operating a personal online account during business
8 hours or while on business property.
- 9 (c) An employer that accesses employee or applicant
10 content for a purpose specified in subsection (b) (3):
- 11 (1) Shall attempt reasonably to limit its access to
12 content that is relevant to the specified purpose;
- 13 (2) Shall use the content only for the specified purpose;
14 and
- 15 (3) Shall not alter the content unless necessary to
16 achieve the specified purpose.
- 17 (d) An employer that inadvertently receives the user name
18 and password, password, or other means of authentication that
19 provides access to an employee's or applicant's personal online
20 account by means of otherwise lawful technology that monitors
21 the employer's network, or employer-provided devices, for a



1 network security, data confidentiality, or system maintenance
2 purpose:

- 3 (1) Is not liable for having the information;
- 4 (2) Shall not use the information to access the personal
5 online account of the employee or applicant or share
6 the information with any other person or entity;
- 7 (3) Shall make a reasonable effort to keep the login
8 information secure;
- 9 (4) Unless otherwise provided in paragraph (5), shall
10 dispose of the information as soon as, as securely as,
11 and to the extent reasonably practicable; and
- 12 (5) Shall, if the employer retains the information for use
13 in connection with the pursuit of a specific criminal
14 complaint or civil action, or the investigation
15 thereof, make a reasonable effort to keep the login
16 information secure and dispose of it as soon as, as
17 securely as, and to the extent reasonably practicable
18 after completing the investigation.

19 (e) Nothing in this chapter shall diminish the authority
20 and obligation of an employer to investigate complaints,
21 allegations, or the occurrence of sexual, racial, or other
22 prohibited harassment under chapter 378.



1 § -4 Protection of student or prospective student online
2 account. (a) Subject to the exceptions in subsection (b), an
3 educational institution shall not:
4 (1) Require, coerce, or request a student or prospective
5 student to:
6 (A) Disclose the user name and password, password, or
7 any other means of authentication, or to provide
8 access through the user name or password, to a
9 personal online account;
10 (B) Disclose the non-public content of a personal
11 online account;
12 (C) Provide password or authentication information to
13 a personal technological device for the purpose
14 of gaining access to a personal online account,
15 or turn over an unlocked personal technological
16 device for the purpose of gaining access to a
17 personal online account;
18 (D) Alter the settings of the personal online account
19 in a manner that makes the content of the
20 personal online account more accessible to
21 others; or



- 1 (E) Access the personal online account in the
2 presence of the educational institution employee
3 or educational institution volunteer, including a
4 coach, teacher, or school administrator, in a
5 manner that enables the educational institution
6 employee or educational institution volunteer to
7 observe the content of the account;
- 8 (2) Require or coerce a student or prospective student to
9 add anyone, including a coach, teacher, school
10 administrator, or other educational institution
11 employee or educational institution volunteer, to the
12 student's or prospective student's list of contacts
13 associated with a personal online account;
- 14 (3) Take, or threaten to take, adverse action against a
15 student or prospective student, including discharge,
16 discipline, prohibition from participation in
17 curricular or extracurricular activities, for failure
18 to comply with an educational institution requirement,
19 coercive action, or request that violates paragraph
20 (1);
- 21 (4) Fail or refuse to admit any prospective student as a
22 result of the prospective student's refusal to



1 disclose any information or take any action specified
2 in paragraph (1).

3 (b) Nothing in subsection (a) shall prevent an educational
4 institution from:

5 (1) Accessing information about a student or prospective
6 student that is publicly available;

7 (2) Complying with a federal or state law, court order, or
8 rule of a self-regulatory organization established by
9 federal or state statute, including a self-regulatory
10 organization as defined in section 3(a)(26) of the
11 Securities Exchange Act of 1934 (15 U.S.C.
12 78c(a)(26));

13 (3) Without requesting or requiring a student or
14 prospective student to provide a user name and
15 password, password, or other means of authentication
16 that provides access to a personal online account,
17 requiring or requesting a student or prospective
18 student to provide specifically identified content
19 that has been reported to the educational institution
20 for the purpose of:

21 (A) Enabling the educational institution to comply
22 with legal and regulatory obligations;



1 (B) Investigating an allegation, based on the receipt
2 of information regarding specifically identified
3 content, of the unauthorized transfer of an
4 educational institution's proprietary or
5 confidential information or financial data to a
6 student's or prospective student's personal
7 online account;

8 (C) Investigating an allegation, based on the receipt
9 of information regarding specifically identified
10 content, of noncompliance with an educational
11 institution prohibition against education-related
12 student misconduct of which the student has
13 reasonable notice, which is in a record, and that
14 was not created primarily to gain access to a
15 personal online account; or

16 (D) Protecting against a threat to safety,
17 educational institution information technology,
18 communications technology systems, or educational
19 institution property;

20 (4) Prohibiting a student or prospective student from
21 using a personal online account for educational
22 institution purposes; or



1 (5) Prohibiting a student or prospective student from
2 accessing or operating a personal online account
3 during school hours or while on school property.

4 (c) An educational institution that accesses student or
5 prospective student content for a purpose specified in
6 subsection (b) (3):

7 (1) Shall attempt reasonably to limit its access to
8 content that is relevant to the specified purpose;

9 (2) Shall use the content only for the specified purpose;
10 and

11 (3) Shall not alter the content unless necessary to
12 achieve the specified purpose.

13 (d) An educational institution that inadvertently receives
14 the user name and password, password, or other means of
15 authentication that provides access to a student's or
16 prospective student's personal online account by means of
17 otherwise lawful technology that monitors the educational
18 institution's network, or educational institution-provided
19 devices, for a network security, data confidentiality, or system
20 maintenance purpose:

21 (1) Is not liable for having the information;



1 (2) Shall not use the information to access the personal
2 online account of the student or prospective student
3 or share the information with any other person or
4 entity;

5 (3) Shall make a reasonable effort to keep the information
6 secure;

7 (4) Unless otherwise provided in paragraph (5), shall
8 dispose of the information as soon as, as securely as,
9 and to the extent reasonably practicable; and

10 (5) Shall, if the educational institution retains the
11 information for use in connection with the pursuit of
12 a specific criminal complaint or civil action, or the
13 investigation thereof, make a reasonable effort to
14 keep the information secure and dispose of it as soon
15 as, as securely as, and to the extent reasonably
16 practicable after completing the investigation.

17 § -5 **Enforcement.** (a) The attorney general may bring a
18 civil action in district court against an employer or
19 educational institution for a violation of this chapter. A
20 prevailing attorney general may obtain:

21 (1) Injunctive and other equitable relief; and



1 (2) A civil penalty of up to \$ for each violation,
2 but not exceeding \$ for all violations caused
3 by the same event.

4 (b) An employee, applicant, student, or prospective
5 student may bring a civil action in district court against the
6 individual's employer or educational institution for a violation
7 of this chapter. A prevailing employee, applicant, student, or
8 prospective student may obtain:

- 9 (1) Injunctive and other equitable relief;
- 10 (2) Actual damages; and
- 11 (3) Costs and reasonable attorney's fees.

12 (c) An employee or agent of an educational institution who
13 violates this chapter may be subject to disciplinary proceedings
14 and punishment. For educational institution employees who are
15 represented under the terms of a collective bargaining
16 agreement, the collective bargaining agreement, any memorandum
17 of agreement or understanding signed pursuant to the collective
18 bargaining agreement, or any recognized and established practice
19 relative to the members of the bargaining unit shall prevail
20 except where the agreement, memorandum, or practice does not
21 conflict with this chapter.



1 (d) An action under subsection (a) shall not preclude an
2 action under subsection (b), and an action under subsection (b)
3 shall not preclude an action under subsection (a).

4 (e) This chapter shall not affect a right or remedy
5 available under law other than this chapter.

6 § -6 Uniformity of application and construction. In
7 applying and construing this chapter, consideration shall be
8 given to the need to promote uniformity of the law with respect
9 to its subject matter among states that enact it.

10 § -7 Relation to Electronic Signatures in Global and
11 National Commerce Act. This chapter modifies, limits, and
12 supersedes the Electronic Signatures in Global and National
13 Commerce Act (15 U.S.C. 7001 et seq.), but does not modify,
14 limit, or supersede section 101(c) of that act (15 U.S.C.
15 7001(c)), or authorize electronic delivery of any of the notices
16 described in Section 103(b) of that act (15 U.S.C. 7003(b)).

17 § -8 Relation to other state laws. Unless otherwise
18 provided in this chapter, if any provision in this chapter
19 conflicts with a provision in any other chapter, the provision
20 in this chapter shall control.

21 § -9 Severability. If any provision of this chapter or
22 its application to any person or circumstance is held invalid,



1 the invalidity does not affect other provisions or applications
2 of this chapter which can be given effect without the invalid
3 provision or application, and to this end the provisions of this
4 chapter are severable."

5 SECTION 2. This Act does not affect rights and duties that
6 matured, penalties that were incurred, and proceedings that were
7 begun before its effective date.

8 SECTION 3. This Act shall take effect on January 7, 2059.



Report Title:

Online Privacy; Employees; Applicants; Students; Prospective Students

Description:

Adopts uniform laws on protecting the online accounts of employees, applicants, students, and prospective students from employers and educational institutions, respectively. (SB429 HD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

