

FIRST REGULAR SESSION

[PERFECTED]

HOUSE COMMITTEE SUBSTITUTE FOR

HOUSE BILL NO. 120

98TH GENERAL ASSEMBLY

0731H.02P

D. ADAM CRUMBLISS, Chief Clerk

AN ACT

To amend chapters 173 and 285, RSMo, by adding thereto two new sections relating to employee password protection.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section A. Chapters 173 and 285, RSMo, are amended by adding thereto two new sections, to be known as sections 173.1600 and 285.045, to read as follows:

173.1600. 1. As used in this section, the following words mean:

(1) "Educational institution" or "school", a private or public institution that offers participants, students, or trainees an organized course of study or training that is academic, technical, trade-oriented, or preparatory for gainful employment in a recognized occupation;

(2) "Personal social media account", an account with an electronic medium or service where users may create, share, and view user-generated content, including, but not limited to, uploading or downloading videos or still photographs, blogs, video blogs, podcasts, messages, emails, or internet website profiles or locations. Personal social media account does not include an account opened at an employer's behest, or provided by an employer, and intended to be used solely on behalf of the employer, or to an account opened at a school's behest, or provided by a school, and intended to be used solely on behalf of the school;

(3) "Prospective student", an applicant for admission to an educational institution;

(4) "Student", any student, participant, or trainee, whether full-time or part-time, in an organized course of study at an educational institution.

2. An educational institution shall not:

EXPLANATION — Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

18 **(1) Require, request, or coerce a student or prospective student to disclose the user**
19 **name and password, password, or any other means of authentication, or provide access**
20 **through the user name or password, to a personal social media account;**

21 **(2) Require, request, or coerce a student or prospective student to access a personal**
22 **social media account in the presence of a school employee or school volunteer, including,**
23 **but not limited to, a coach, teacher, or school administrator, in a manner that enables the**
24 **school employee or school volunteer to observe the contents of such account; or**

25 **(3) Compel a student or prospective student to add anyone, including a coach,**
26 **teacher, school administrator, or other school employee or school volunteer, to his or her**
27 **list of contacts associated with a personal social media account or require, request, or**
28 **otherwise coerce a student or prospective student to change the settings that affect a third**
29 **party's ability to view the contents of a personal social media account.**

30 **3. An educational institution shall not:**

31 **(1) Take any action or threaten to take any action to discharge, discipline, prohibit**
32 **from participating in curricular or extracurricular activities, or otherwise penalize a**
33 **student for a student's refusal to disclose any information specified in subdivision (1) of**
34 **subsection 2 of this section, for refusal to take any action specified in subdivision (2) of**
35 **subsection 2 of this section, or for refusal to add a coach, teacher, school administrator, or**
36 **other school employee or school volunteer to his or her list of contacts associated with a**
37 **personal social media account or to change the settings that affect a third party's ability**
38 **to view the contents of a personal social media account, as specified in subdivision (3) of**
39 **subsection 2 of this section; or**

40 **(2) Fail or refuse to admit any prospective student as a result of the prospective**
41 **student's refusal to disclose any information specified in subdivision (1) of subsection 2 of**
42 **this section, for refusal to take any action specified in subdivision (2) of subsection 2 of this**
43 **section, or for refusal to add a coach, teacher, school administrator, or other school**
44 **employee or school volunteer to his or her list of contacts associated with a personal social**
45 **media account or to change the settings that affect a third party's ability to view the**
46 **contents of a personal social media account, as specified in subdivision (3) of subsection 2**
47 **of this section.**

48 **4. Nothing in this section prevents an educational institution from:**

49 **(1) Accessing information about a student or prospective student that is publicly**
50 **available;**

51 **(2) Complying with state and federal laws, rules, and regulations and the rules of**
52 **self-regulatory organizations, where applicable;**

53 **(3) Requesting or requiring a student or prospective student to share specific**
54 **content that has been reported to the school, without requesting or requiring a student or**
55 **prospective student to provide a user name and password, password, or other means of**
56 **authentication that provides access to a personal social media account, as part of:**

57 **(a) An investigation for the purpose of ensuring compliance with applicable laws**
58 **or regulatory requirements;**

59 **(b) An investigation of actual disruption to school functions based on receipt of**
60 **specific information about the unlawful harassment or bullying of a student by the student**
61 **or prospective student from whom the content is requested or required;**

62 **(4) Prohibiting a student or prospective student from using a personal social media**
63 **account for school purposes; or**

64 **(5) Prohibiting a student or prospective student from accessing or operating a**
65 **personal social media account during school hours or while on school property.**

66 **5. If a school inadvertently receives the user name and password, password, or**
67 **other means of authentication that provides access to a personal social media account of**
68 **a student or prospective student through the use of an otherwise lawful virus scan or**
69 **firewall that monitors the school's network or school-provided devices, the school is not**
70 **liable for having the information but shall not use the information to access the personal**
71 **social media account of the student or prospective student or share the information with**
72 **anyone, and shall delete the information immediately, if reasonably practicable.**

73 **6. It shall be an unlawful employment practice for an educational institution to**
74 **violate the provisions of this section. A student or prospective student may bring a cause**
75 **of action for general or specific damages based on any violation of this section.**

285.045. 1. This section shall be known and may be cited as "The Password
2 **Privacy Protection Act".**

3 **2. As used in this section, the following terms shall mean:**

4 **(1) "Applicant", any person applying for employment;**

5 **(2) "Electronic communications device", any device that uses electronic signals to**
6 **create, transmit, and receive information which shall include, but not be limited to,**
7 **computers, telephones, personal digital assistants, and other similar devices;**

8 **(3) "Employee", any person performing work or service of any kind or character**
9 **for hire within the state of Missouri, including independent contractors;**

10 **(4) "Employer", any person or entity employing any person for hire within the**
11 **state of Missouri, including a public employer;**

12 **(5) "Employment", the act of employing or state of being employed, engaged, or**
13 **hired to perform work or services of any kind or character within the state of Missouri;**

14 **(6) "Personal online account", an online account that is used by an employee or**
15 **applicant exclusively for personal communications unrelated to any business purposes of**
16 **the employer. Such account shall not include any account created, maintained, used, or**
17 **accessed by an employee or applicant for business related communications or for a**
18 **business purpose of the employer;**

19 **(7) "Personal online service", an online service that is used by an employee or**
20 **applicant exclusively for personal communication or use unrelated to any business**
21 **purposes of the employer. Such service shall not include any service maintained, used, or**
22 **accessed by an employee or applicant for business related communications or uses or for**
23 **a business purpose of the employer;**

24 **(8) "Political subdivision", any agency of the state, county, city, town, township,**
25 **village, special district or subdistrict, or any unit of the state authorized to levy taxes;**

26 **(9) "Public employer", every department, agency, or instrumentality of the state**
27 **or political subdivision of the state;**

28 **(10) "Work", any job, task, labor, services, or any other activity for which**
29 **compensation is provided, expected, or due.**

30 **3. Subject to the exceptions provided in subsection 4 of this section, an employer**
31 **shall not request or require an employee or applicant to disclose any user name, password,**
32 **or other authentication means for accessing any personal online account or personal online**
33 **service or compel an employee or applicant for employment to add the employer or an**
34 **employment agency to the employee's or applicant's list of contacts associated with a**
35 **personal internet account.**

36 **4. An employer may request or require an employee to disclose any user name,**
37 **password, or other authentication means for accessing:**

38 **(1) Any electronic communications device supplied by or paid for in whole or in**
39 **part by the employer;**

40 **(2) Any accounts or services provided by the employer;**

41 **(3) Any accounts or services the employee uses for business purposes; or**

42 **(4) Any accounts or services used as a result of the employee's employment**
43 **relationship with the employer.**

44 **5. An employer shall not:**

45 **(1) Discharge, discipline, or otherwise penalize or threaten to discharge, discipline,**
46 **or otherwise penalize an employee solely for an employee's refusal to disclose any**
47 **information specified in subsection 3 of this section;**

48 **(2) Fail or refuse to hire any applicant as a result of the applicant's refusal to**
49 **disclose any information specified in subsection 3 of this section; or**

50 **(3) Be held liable for failure to request or require that an applicant or employee**
51 **disclose any information specified in subsection 3 of this section.**

52 **6. An employee shall not transfer an employer's proprietary or confidential**
53 **information or financial data to an employee's personal online account or personal online**
54 **service without the employer's authorization.**

55 **7. This section shall not be construed to prevent an employer from engaging in any**
56 **of the following activities:**

57 **(1) Conducting an investigation for the purposes of ensuring compliance with**
58 **applicable laws or regulations against work-related employee misconduct based on the**
59 **receipt of specific information about activity on a personal online account or personal**
60 **online service by an employee or other source;**

61 **(2) Conducting an investigation of an employee's actions based on the receipt of**
62 **specific information about the unauthorized transfer of an employer's proprietary**
63 **information, confidential information or financial data to a personal online account or**
64 **personal online service by an employee or other source;**

65 **(3) Conducting an investigation as specified in subdivision (1) or (2) of this**
66 **subsection that requires the employee's cooperation to share the content that has been**
67 **reported in order to make a factual determination;**

68 **(4) Disciplining or discharging an employee for transferring the employer's**
69 **proprietary or confidential information or financial data to an employee's personal**
70 **internet account without the employer's authorization;**

71 **(5) Restricting or prohibiting an employee's access to certain websites while using**
72 **an electronic communications device that is paid for in whole or in part by the employer**
73 **or while using an employer's network or resources, in compliance with state and federal**
74 **law; or**

75 **(6) Monitoring, reviewing, accessing, or blocking electronic data stored on an**
76 **electronic communications device that is paid for in whole or in part by the employer, or**
77 **such data that is traveling through or stored on an employer's network, in compliance with**
78 **state and federal law.**

79 **8. This act shall not prohibit or restrict any employer from viewing, accessing, or**
80 **utilizing information about any employee or applicant that can be obtained without the**
81 **information specified in subsection 3 of this section or that is available to the public.**

82 **9. This act shall not be construed to prevent an employer from complying with state**
83 **or federal laws or regulations or the rules of self-regulatory organizations as that term is**
84 **defined in 15 U.S.C. Section 78c(a)(26).**

85 **10. This act shall not be construed to prohibit an employer from requesting an**
86 **employee to provide an email address in order to conduct business-related communications**
87 **with the employee. However, such address shall not be disclosed to any third party.**

✓