SECOND REGULAR SESSION

HOUSE BILL NO. 1358

99TH GENERAL ASSEMBLY

INTRODUCED BY REPRESENTATIVE DAVIS.

4168H.01I D. ADAM CRUMBLISS, Chief Clerk

AN ACT

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

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 terms mean:

(1) "Educational institution" or "school", a public or private institution of higher education or a public or private school giving instruction in a grade or grades not higher than the twelfth grade 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, videos or still photographs, blogs, video blogs, podcasts, messages, emails, or internet website profiles or locations. The term "personal social media account" does not include:

(a) 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

(b) 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;

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.

(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:

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

(2) Except as provided under subsection 4 of this section, require, request, or coerce a student or prospective student to access a personal social media account in the presence of a school employee or school volunteer including, but not limited to, a coach, teacher, or school administrator, in a manner that enables the school employee or school volunteer to observe the contents of such account; or

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

3. An educational institution shall not:

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

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

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

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

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

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

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

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

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

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

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

6. It shall be an unlawful employment practice for an educational institution to violate the provisions of this section. A student or prospective student may bring a cause 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 Privacy Protection Act".

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

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

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

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

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

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

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

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

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

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

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

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

4. An employer may request or require an employee to disclose any username, password, or other authentication means for accessing:

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

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

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

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

5. An employer shall not:

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

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

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

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

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

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

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

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

(4) Disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal online account or personal online service without the employer's authorization;

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

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

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

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

10. This section shall not be construed to prohibit an employer from requesting an employee to provide an email address in order to conduct business-related communications with the employee. An employer who makes this request shall not disclose such address to any third party unless the employee authorizes the disclosure; except that, nothing in this section shall prevent an employer from disclosing an employer-provided email address to any third party.

✓