HB 1332

Department of Legislative Services

Maryland General Assembly
2013 Session

FISCAL AND POLICY NOTE

House Bill 1332 (Delegate Tarrant, *et al.*)
Appropriations

Educational Institutions - Personal Electronic Account - Privacy Protections

This bill prohibits an educational institution from requiring, requesting, suggesting, or causing a student or a prospective student to grant access to, allow observation of, or disclose information that allows access to or observation of the individual's personal electronic account, not including any assessable communication. In addition, an educational institution is prohibited from compelling a student or an applicant, as a condition of acceptance or participation in curricular or extracurricular activities, to (1) add anyone including specified individuals to the list of contacts associated with a personal electronic account or (2) require, request, suggest, or cause a student or an applicant to change the privacy settings associated with a personal electronic account. An educational institution may not penalize a student for refusing to disclose any of the specified information or add anyone to their account.

The bill takes effect July 1, 2013.

Fiscal Summary

State Effect: Meeting the requirements of the bill does not impact public four-year institutions of higher education or Baltimore City Community College finances.

Local Effect: Meeting the requirements of the bill does not impact local school system or community college finances.

Small Business Effect: Minimal.

Analysis

Bill Summary: "Educational institution" is defined as a public or private educational 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.

In the bill, "personal electronic account" does not include an account that is opened on behalf of, or owned or provided by, an educational institution.

The bill does not prohibit a student or an applicant from allowing athletic coaches or administrators to view the student's or the applicant's publicly accessible communications.

The bill does not apply to suspected criminal activity investigations performed by a public safety department or police agency of an educational institution into an applicant's or a student's publicly accessible communications. The bill also does not apply to an investigation in accordance with the health or public safety assessment policy or protocol of an educational institution into an applicant's or student's publicly accessible communications.

Further, the bill does not prohibit or restrict an educational institution from viewing, accessing, or utilizing information about a student or applicant that may be obtained without any required access information or is available in the public domain. However, the bill does not create a duty for an educational institution to search or monitor the activity of a personal electronic account.

An educational institution is not liable under the bill for a failure to request or require that a student or a prospective student grant access to, allow observation of, or disclose information that allows access to or observation of the individual's personal electronic account.

By December 1 of each year, an educational institution must report any violation of the bill to the Senate Education, Health, and Environmental Affairs Committee and the House Ways and Means Committee.

Current Law: State law does not specifically address privacy issues related to a student's, or an applicant's, personal user name and password information.

An employer, including the State and local governments, is prohibited from requesting or requiring an employee or applicant for employment to disclose a user name, password, or other means of accessing an Internet site or electronic account. An employer may not

penalize an employee or applicant for employment for refusing to disclose this information.

An "institution of postsecondary education" is defined as a school or other institution that offers an educational program in the State for individuals who are age 16 or older and who have graduated from or left elementary or secondary school.

Background: In 2011 the University of North Carolina (UNC) updated its Department of Athletics Policy on Student-Athlete Social Networking and Media Use. The policy requires each team to "identify at least one coach or administrator who is responsible for having access to and regularly monitoring the content of team members' social networking sites and postings." The policy was apparently in response to a National Collegiate Athletic Association (NCAA) Notice of Allegation (NOA) that alleged among other things that the institution failed to "monitor social networking activity that visibly illustrated potential amateurism violations within the football program, which delayed the institution's discovery and compounded the provision of impermissible benefits..." The NCAA investigation was apparently triggered by the "tweets" from a former UNC football star.

Despite the NOA, NCAA reports it does not require its members to monitor the social media activity of its members; however, it does encourage institutions to do so. A few entrepreneurs have seen this as a business opportunity, but some legal experts warn that monitoring student-athletes' accounts could expose the schools to litigation.

There are now a few companies that will monitor the Twitter, Facebook, and other social media accounts of student-athletes for a fee. In general, the companies monitor the social media activity by installing monitoring software on student-athletes' electronic devices. More than two dozen institutions, including the University of Louisville, Louisiana State University, and Texas A&M, have signed up with a social media monitoring company. According to the *Washington Post*, monitoring companies have approached several Maryland institutions, although none has signed up with a company yet.

Some legal experts say that monitoring student-athletes' social media activity at public institutions could violate the Fourth Amendment of the U.S. Constitution that protects students from unreasonable searches and seizures. Other legal experts warn if a university athletic department does choose to actively monitor its students' social media accounts and fails to recognize or act on information that could have predicted or prevented property damage, personal injury, or death, then the school could be sued for negligence or dereliction of duty. On the other hand, acting too quickly on such information could result in a student filing a claim against the school for reputational damage or lost future financial benefits. Finally, an institution could be accused of

discrimination or violating a student's Fourteenth Amendment right of equal protection based on how it determines which students to monitor.

In October 2011, the University of Maryland, College Park issued social media guidelines for its more than 700 student-athletes. The guidelines remind student-athletes to think before using slurs about race, religion, or sexual orientation; to follow NCAA rules; and to monitor comments for offensive language.

The Maryland State Department of Education (MSDE) reports that it adheres to the Family Educational Rights and Privacy Act, a federal law that protects the privacy of student and family information. In addition, MSDE follows guidelines specified by the Maryland Department of Information Technology's information security policy.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Baltimore City Community College, Maryland State Department of Education, Maryland Higher Education Commission, University System of Maryland, *The Washington Post*, *Carolina March*, *Fox Sports*, Department of Legislative Services

Fiscal Note History: First Reader - March 3, 2013
ncs/rhh

Analysis by: Caroline L. Boice

Direct Inquiries to:
(410) 946-5510
(301) 970-5510