Government of the District of Columbia
Office of the Chief Financial Officer

Jeffrey S. DeWitt
Chief Financial Officer

MEMORANDUM

TO:	**The Honorable Phil Mendelson** **Chairman, Council of the District of Columbia**
FROM:	**Jeffrey S. DeWitt** **Chief Financial Officer**
DATE:	**October 4, 2016**
SUBJECT:	**Fiscal Impact Statement – Protecting Student's Digital Privacy Act of 2016**
REFERENCE:	**Bill 21-578, Committee Print as shared with the Office of Revenue Analysis on October 3, 2016**

Conclusion

Funds are sufficient in the fiscal year 2017 through fiscal year 2020 budget and financial plan to implement the bill.

Background

The bill establishes privacy and accessibility guidelines for student information, school issued electronic devices, and student personal media accounts. Below is a summary of the key changes included in the bill.

Student Personal Information Security

The bill requires operators of educational web sites, online services, online applications, and mobile applications to implement and maintain security policies that protect student information. Operators must notify students, parents, educational institutions, and local education agencies (LEAs) if unauthorized access of student information occurs. Any student information submitted to an operator is considered under the control of an LEA and must be deleted if service is terminated or completed.

The bill prohibits operators from:

- selling, renting, or trading personally identifiable student information unless the operator is acquired by another entity or if a student has given consent to the operator;
- conducting targeted advertisements based on student information;

- using data to develop, in full or in part, a profile of a student or group of students; and,
- disclosing personally identifiable student information.

The bill allows operators to:

- use personally identifiable student information internally to maintain, develop, support, improve, or diagnose an operator's grades pre-k through 12 site, service, or application;
- use personally identifiable student information for adaptive learning or customized student learning purposes;
- use, share, and sell student information if the personally identifiable information has been deleted;
- use its grades pre-k through 12 site, service, or application to recommend products, content, or services to a student related to educational, learning, or employment opportunities;
- respond to a student's request for information or feedback; and,
- market products directly to parents if the marketing did not result from the use of personally identifiable student information obtained by the operator.

Privacy of School Issued Electronic Devices

The bill establishes the terms under which school-based personnel are prohibited from accessing data on school-issued electronic devices. Specifically, school-based personnel are prohibited from analyzing, sharing, or transferring a student's browser history, key stroke history, and location history. School-based personnel can only access this information if:

- data will be used for educational purposes;
- there is a reasonable suspicion that a student has violated institutional policy;
- doing so is necessary to update a device's software or security;
- doing so is necessary to respond to an imminent threat to life or safety; or,
- data is posted on an electronic medium accessible by the general public or school-based personnel.

The bill prohibits school-based personnel from tracking a student's electronic device in real-time or accessing historic tracking data unless:

- the phone is reported stolen;
- a judge issues a warrant to track a phone; or,
- an imminent threat to life or safety exists.

If a student's location tracking is accessed, the educational institution must provide notice to the student's parents, within 72-hours, stating why the data was accessed.

The bill prohibits school-based personnel from accessing audio or video functions on a student's device unless:

- a student initiates video or audio;
- the activation is ordered by a judge; or,
- there is an imminent threat to life or safety.

If a student's audio and video functions are accessed, the educational institution must provide notice to the student's parents stating why the data was accessed within 72-hours.

The bill requires educational institutions to erase all data stored on an electronic device as soon as the student permanently returns the device.

Privacy of Student Personal Accounts and Devices

The bill prohibits school-based[1] personnel from taking action against a student because he or she would not disclose their private personal media account information. This includes a student's username, password, and account authentication information. The bill requires educational institutions and school-based personnel to delete inadvertently received student personal media account usernames, passwords, and other authentication information as soon as possible.

The bill allows school-based personnel to access a student's personal media account if the student is suspected of using the account in violation of an institution's policy. A device may only be searched if it is located and is accessible on school property. School-based personnel must notify the student and student's parent and document reasonable suspicion in order to access a student's personal media account. No information may be shared with persons that are unrelated to an investigation unless an immediate threat exists. If a student's personal media account is searched, the educational institution must provide notice to the student's parent stating why the account was accessed within 72-hours.

Financial Plan Impact

Funds are sufficient in the fiscal year 2017 through fiscal year 2020 budget and financial plan to implement the bill. Instituting privacy guidelines for personal student data, devices, and personal media accounts will not require additional resources.

[1] "School-based personnel" are employees or volunteers of an educational institution or employees of an entity with whom the educational institution contracts, who acts as an agent of the educational institution.