Councilmember David Grosso

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To require that any contract or agreement between a local education agency and a student information system provider shall expressly authorize and require the provider to establish, implement, and maintain appropriate security measures to protect student data and personally identifiable student information and to comply with certain procedures with regard to accessing, analyzing, storing, or sharing student information; to prohibit an educational institution or 1-to-1 device provider that provides a technological device to a student for overnight or home use from accessing or tracking the device, the activity or data, either remotely or in person, except in limited circumstances; to prohibit an educational institution from requiring or coercing a student or prospective student to disclose the user name and password to a personal social media account, add anyone to their list of contacts associated with a personal social media account or to change the settings that affect a third party's ability to view; to prohibit an educational institution from taking action or threatening to take action to discipline, expel, unenroll, prohibit from participating in curricular or extracurricular activities, or otherwise penalize a student for a student's refusal to disclose personal social media account information; and to prohibit school employees from accessing or compelling a student to produce, display, share or provide access to, any data or other content input into, stored upon, or accessible from a student's personal technological device, even when the personal technological device is being carried or used in violation of an educational institution policy, except for in limited circumstances.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Protecting Students Digital Privacy Act of 2016".

Sec. 2. Definitions.

For the purposes of this act, the term:

(1) "1-to-1 device" means a technological device provided to a student pursuant to a 1-to-1 program.

(2) "1-to-1 device provider" means a person, entity, or agent thereof, that provides a 1-to-1 device to a student or educational institution pursuant to a 1-to-1 program, and includes any business or non-profit entities that share a parent or, subsidiary, or relationship with the entity that provides the 1-to-1 device.

(3) "1-to-1 program" means any program authorized by an educational institution where a technological device is provided to a student by or through an educational institution for overnight or at-home use.

(4) "Educational institution" means a public school or public charter school in the District of Columbia.

(5) "Education research" means the systematic gathering of empirical information to advance knowledge, answer questions, identify trends, or improve outcomes within the field of education.

(6) "Local education agency" or "LEA" means the District of Columbia Public Schools system or any individual or group of public charter schools operating under a single charter.

(7) "Location tracking technology" means any hardware, software, or application that collects or reports data that identifies the geophysical location of a technological device.

(8) "Opt-in agreement" means a discrete, verifiable, written or electronically generated agreement by which, subject to the provisions of this act, a student or the student's parent or legal guardian voluntarily grants school-based personnel, SIS provider, or 1-to-1 device provider with limited permission to access and interact with a specifically defined set of personally identifiable student information.

(9) "OSSE" means the Office of the State Superintendent for Education.

(10) "Personal social media account" means 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, e-mails, or Internet website profiles or locations. Personal social media account does not include an account opened at an educational institution's behest, or provided by an educational institution, and intended to be used solely on behalf of the educational institution.

(11) "Personal technological device" means a technological device owned, leased, or otherwise lawfully possessed by a student that is not a 1-to-1 device.

(12) "Personally identifiable student information" means one or more of the following:

(1) A student's name;

(2) The name of a student's parent, legal guardian, or other family member;

(3) The address of a student or student's parent, legal guardian, or other family member;

(4) A photograph, video, or audio recording that contains the student's image or voice;

(5) Indirect identifiers, including but not limited to a student's date of birth, place of birth, mother's maiden name, social security number, student number, telephone number, credit card account number, insurance account number, financial services account number, customer number, email address, social media address, or other electronic address;

(6) Any aggregate or de-identified student data that is capable of being de-aggregated or reconstructed to the point that individual students can be identified; and

(7) Any student data or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify a specific student with reasonable certainty.

(13) "School-based personnel" means any individuals employed by an educational institution whether on a regular full-time basis, an hourly basis, or otherwise that has interaction with students. This includes individuals employed by a person or entity contracted with by an educational institution to provide school-based services as an agent of the educational institution.

(14) "Student information system" or "SIS" means a software application or cloud-based service that allows an education institution to input, maintain, manage, or retrieve student data or personally identifiable student information, including applications that track or share personally identifiable student information in real time.

(15) "Student information system provider" or "SIS provider" means an entity that sells, leases, providers, operates, or maintains a student information system for the benefit of a LEA or educational institution.

(16) "Technological device" means any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device that can be used for creating, storing, or transmitting information in the form of electronic data.

Sec. 3. Student information systems.

(a) Any contract or other agreement between a local education agency and an SIS provider pursuant to which the SIS provider sells, leases, provides, operates, or maintains a student information system for the benefit of the LEA:

(1) Shall expressly authorize and require the SIS provider to:

(A) Establish, implement and maintain appropriate security measures, consistent with best current practices, to protect the student data and personally identifiable student information the SIS provider creates, sends, receives, stores, and transmits in conjunction with the operation of the student information system;

(B) Acknowledge that no data stored on the student information system is the property of the SIS provider;

(C) Establish and implement policies and procedures for responding to data breaches involving the unauthorized acquisition of or access to any personally identifiable student information on the student information system. Such policies and procedures, at a minimum, shall:

(i) Require notice be provided by the SIS provider to any and all affected parties, including education institutions, students, and students' parents and legal guardians, within 30 days of the discovery of the breach;

(ii) Require the notice to include a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(iii) Require the notice to provide a procedure by which affected parties may learn what types of sensitive personally identifiable information the SIS provider maintained about the affected individual; and

(iv) Satisfy all other applicable breach notification standards established under state or federal law.

(2)(A) Permanently delete all data stored on the student information system, and destroy all non-digital records containing any personally identifiable student information

retrieved from the student information system, within 90 days of the termination of the SIS provider's contact with the LEA, except where the SIS provider and the person(s) authorized to sign a valid opt-in agreement pursuant to this section, mutually agree the SIS provider will retain specifically identified data and/or non-digital records for the student's benefit.

(B) Prior to deletion, if requested by the educational institution, the terminated SIS provider shall transfer a designated portion or all of the data stored on the student information system to another designated SIS provider at the educational institution's expense.

(3) Comply with all the applicable obligations and restrictions established for SIS providers in this act.

(b) Shall expressly prohibit the SIS provider from:

(1) Analyzing, interacting with, sharing, or transferring any student data or personally identifiable student information the LEA inputs into or otherwise provides to the student information system unless:

(A) Permission to do so has been granted, pursuant to an opt-in agreement;

(B) The SIS provider analyzes or interacts with the student data or personally identifiable student information in order to meet a contractual obligation to the LEA and any analysis of or interaction with the data or information is limited to meeting that contractual obligation;

(C) The SIS provider analyzes or interacts with the student data or personally identifiable student information in response to a specific request made by an educational institution and any data or information produced as a result of the analysis or interaction is limited to the educational purpose for which it was sought;

(D) The LEA determines, and documents in writing, that sharing specific student data or personally identifiable student information is necessary to safeguard students' health and/or safety while students are traveling to or from the educational institution, are on the educational institution's property, or are participating in an event or activity supervised by the educational institution;

(E) At the request of the LEA, the SIS provider de-identifies and/or aggregates student data or personally identifiable student information for the purpose of enabling the LEA to comply with federal or District reporting and data sharing requirements or education research; or

(F)(1) The data is accessed by the SIS provider for the exclusive purpose of testing and improving the value and performance of its student information system for the benefit of the educational institution.

(2) Where data is accessed to test and improve student information system value and performance:

(i) Any copied data shall be permanently deleted within 60 days of the date the copy was created; and

(ii) Any data analysis that contains personally identifiable student information shall be permanently deleted within 60 days of the date the analysis was created.

(2)(A) Selling any student data or personally identifiable student information stored on or retrieved from the student information system unless it is sold as part of a sale or merger of the entirety of the SIS provider's business.

(B) Upon such a sale or merger, the provisions of this act, and any relevant contracts or agreements, shall apply fully to the new purchasing or controlling person or entity;

(3) Using any student data or personally identifiable student information stored on or retrieved from the student information system to inform, influence or guide marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement; or

(4) Using any student data or personally identifiable student information stored on or retrieved from the student information system to develop, in full or in part, a profile of a student or group of students for any commercial or other non-educational purposes.

(c) Subject to written authorization from the LEA, school-based personnel may access and interact with student data and personally identifiable student information on a student information system in furtherance of their professional duties.

(d) Notwithstanding any other provisions in this section, no employee of an LEA may receive authorization to access and interact with student data or personally identifiable student information on a student information system until the employee has received adequate training to ensure the employee's understanding and compliance with the provisions of this section.

(e) Employees of an LEA, including school-based personnel, may not sell, share, or otherwise transfer student data or personally identifiable student information to another person or entity, except:

(1) Where specifically authorized to do so pursuant to this section;

(2) With the educational institution that employees the school employee;

(3) With another school employee who is eligible to access such information; and

(4) Where:

(i) The school employee is a teacher;

(ii) The teacher is transferring student data to a software application for classroom recordkeeping or management purposes only and any third parties with access to the software application are expressly prohibited from reviewing or interacting with the transferred data.

(f)(1) A student's parent or guardian, upon written request to an educational institution or LEA, shall be permitted to inspect and review their child's student data and personally identifiable student information that is stored on a student information system. LEAs shall afford parents and legal guardians a reasonable and fair opportunity to request corrections to or seek removal of inaccurate data.

(2) The right of a student's parent or guardian to review their child's student data and personally identifiable student information shall not apply where:

(A) Such information was supplied by the child to the educational institution; and

(B) There is a reasonable likelihood the disclosure of such information would generate a threat to the student's health or safety.

(3) The right of a student's parent or guardian to review their child's student data and personally identifiable student information shall not apply where access to particularly specified information has been waived by the student or the student's parent or guardian.

(4) A LEA shall establish appropriate procedures for:

(A) Reviewing and responding to requests made pursuant to paragraph (m) within 30 days of its receipt of the request; and

(B) Requesting and receiving a fair hearing in the event a requested correction is denied.

(g)(1) One year after a student's graduation, withdrawal, or expulsion from a LEA, all student data and personally identifiable student information related to that student that is stored in a student information system shall be deleted.

(2) This provision shall not apply to:

(A) A student's name and social security number;

(B) A student's transcript, graduation record, letters of recommendation, and other information required by an institution of higher education for an application for admission or by a potential employer for an application for employment;

(C) Student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(D) De-identified student data that is being retained at the request of the educational institution for the purpose of educational research or analysis; and

(E) Student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant.

(h)(1) Within 180 days of receiving notification of a student's graduation, withdrawal, or expulsion from a LEA, all physical or digital copies of any student data and personally identifiable student information related to the student that was obtained from a student information system and is in the possession or under the control of an SIS provider or other third party shall be deleted or destroyed.

(2) This provision shall not apply to:

(A) Student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(B) Aggregated or de-identified student data obtained for the purpose of education research;

(C) Student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant; and

(D) Specifically identified student data or personally identifiable student information, where:

(i) Its retention is requested by the person(s) authorized to sign a valid opt-in agreement pursuant to section 4 of this act; and

(ii) The SIS provider and LEA voluntarily consent to its retention.

(i) Within 90 days of a student's graduation, withdrawal, or expulsion from an education institution, notice of such shall be provided by the educational institution to the SIS provider, which shall in turn notify any third parties with whom the SIS provider shared the student's student data or personally identifiable student information.

(j) No person or entity, other than an educational institution, school-based personnel or SIS provider, other than as provided for in this section, shall be granted access to review or interact with a student information system and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or as part of an audit initiated by an educational institution or OSSE.

(k) Nothing in the section shall be read to prohibit an educational institution from providing directory information to a vendor for the express purpose of providing photography

services, class ring services, yearbook or student publication publishing services, memorabilia services, or similar services, provided the vendor agrees in writing:

(1) Not to sell or transfer the data to any other persons or entities;

(2) To use the data solely for the express purpose for which it was provided; and

(3) To destroy the data upon completion of its use for the express purpose it was provided.

(l) Nothing in this section shall be read to supersede or otherwise limit any laws that provide enhanced privacy protections to students or further restrict access to their educational records or personally identifiable student information.

Sec. 4. Opt-In agreements for student information systems.

(a) Notwithstanding any other section of this act, a valid opt-in agreement for student information systems shall identify, with specificity:

(1) The precise subset of personally identifiable student information in the student information system (e.g., student attendance records, student disciplinary records) as to which the SIS provider is being granted authority to access, analyze, interact with, share or transfer;

(2) The name of the SIS provider(s) to whom the authority to access, analyze, interact with, share and/or transfer personally identifiable student information in the student information system is being granted;

(3) The educational purpose(s) for which the authority to access, analyze, interact with, share and/or transfer personally identifiable student information is being granted; and

(4) The individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall only be valid if it has been signed by:

(1) The student's parent or guardian, if the student is in elementary school;

(2) The student and the student's parent or legal guardian, if the student has advanced beyond elementary school but is not 18 years of age or older; or

(3) The student alone, if the student is 18 years of age or older.

(c) A valid opt-in agreement may authorize an SIS provider to share or transfer personally identifiable student information to another person or entity only where:

(1) The purpose of the transfer of the personally identifiable student information is to benefit:

(A) The operational, administrative, analytical, or educational functions of the LEA, including education research; or

(B) The student's education.

(2) The subset of personally identifiable student information to be shared or transferred is identified with specificity in the opt-in agreement;

(3) The person or entity to whom the personally identifiable student information is being shared or transferred is identified with specificity in the opt-in agreement;

(4) The benefit to the LEA or student is identified with specificity in the opt-in agreement; and

(5) For each student, a record of what specific personally identifiable student information pertaining to that student was shared or transferred, when it was shared or transferred, and with whom it was shared or transferred is appended to the student's record.

(d) Any person or entity that accesses or takes possession of any student data or personally identifiable student information pursuant to section 2(b)(2)(A) of this act shall be subject to same restrictions and obligations under this Section as the SIS provider from which the student data or personally identifiable student information was obtained.

(e) An opt-in agreement shall not be valid if it grants general authority to access, analyze, interact with, share or transfer a student's personally identifiable student information in a student information system.

(f) Except as authorized in this section, no SIS provider, school-based personnel, or other person or entity who receives personally identifiable student information, directly or indirectly, from a student information system pursuant to an opt-in agreement may share, sell or otherwise transfer such information to another person or entity.

(g) An opt-in agreement may be revoked at any time, upon written notice to an LEA or educational institution, by the person(s) eligible to authorize an opt-in agreement pursuant to this section. Within 30 days of such a revocation, notice to the SIS provider shall be provided by the LEA.

(h) An SIS provider that accesses, analyzes, interacts with, shares or transfers personally identifiable student information to another person or entity shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(i) No educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement.

Sec. 5. 1-to-1 Programs.

(a) Where an educational institution or 1-to-1 device provider provides a student with a technological device pursuant to a 1-to-1 program, no school-based personnel or 1-to-1 device provider may access or track such a device or the activity or data thereupon, either remotely or in person, except in accordance with the provisions of this section.

(b) School-based personnel or 1-to-1 device provider shall not access, analyze, share, or

transfer any data input into, stored upon, or sent or received by a student's 1-to-1 device, including but not limited to its browser history, key stroke or location history unless:

(1) The data being collected is not personally identifiable student information;

(2) The data is being accessed by or on behalf of school-based personnel who:

(A) Is the student's teacher;

(B) Is receiving or reviewing the information for an educational purpose consistent with the school-based personnel's professional duties; and

(C) Does not use the information, or permit any other person or entity to use the information, for any other purpose;

(3) School-based personnel or 1-to-1 device provider has been authorized to access specific personally identifiable student information pursuant to an opt-in agreement;

(4) School-based personnel has a reasonable suspicion that the student has violated or is violating an educational institution policy and a reasonable suspicion that the data on the 1-to-1 device contains evidence of the suspected violation, subject to the following limitations:

(A) Prior to searching a student's 1-to-1 device based on reasonable suspicion, the school-based personnel shall document the reasonable suspicion and notify the student and the student's parent or legal guardian of the suspected violation and what data will be accessed in searching for evidence of the violation;

(B) An educational institution, subject to any other relevant legal restrictions, may seize a student's 1-to-1 device to prevent data deletion pending notification, provided that:

(i) The pre-notification seizure period is no greater than 48 hours; and

(ii) The 1-to-1 device is stored securely on educational institution property and not accessed during the pre-notification seizure period;

(C) The search shall be strictly limited to components of the device or data on the device reasonably likely to yield evidence of the suspected policy violation. No person shall be permitted to copy, share, or transfer any data or any information obtained pursuant to a search under this subsection that is unrelated to the suspected violation that prompted the search; and

(D) Where a student is suspected of illegal conduct, no search of the 1-to-1 device may occur unless a judicial warrant has been secured in accordance with subparagraph (b)(5) of this section, even if the student is also suspected of a related or unrelated violation of educational institution policy;

(5) School-based personnel or a law enforcement official reasonably suspects the student has engaged or is engaging in illegal conduct, reasonably suspects data on the 1-to-1 device contains evidence of the suspected illegal conduct, and has secured a judicial warrant for a search of the device;

(6) Doing so is necessary to update or upgrade the 1-to-1 device's software, or to protect the device from cyber-threats, and access is limited to that purpose;

(7)(A) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose.

(B) Within 72 hours of accessing a 1-to-1 device's data in response to an imminent threat to life or safety, the school-based personnel or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or

legal guardian, and the educational institution with a written description of the precise threat that prompted the access and what data was accessed; or

(8) The accessed data is otherwise posted on a website that:

(A) Is accessible by the general public; or

(B) Is accessible by school-based personnel who are granted permission to view the content.

(c) School-based personnel or 1-to-1 device provider shall not use a student's 1-to-1 device's location tracking technology to track a device's real-time or historical location, unless:

(1) The student to whom the device was provided, or the student's parent or legal guardian, has notified school-based personnel or law enforcement official that the device is missing or stolen;

(2) Such use is ordered pursuant to a judicial warrant; or

(3)(A) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose; and

(B) Within 72 hours of accessing a 1-to-1 device's location tracking technology is accessed in response to an imminent threat to life or safety, the school-based personnel or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data and features were accessed.

(d) School-based personnel or 1-to-1 device provider shall not activate or access any audio or video receiving, transmitting, or recording functions on a student's 1-to-1 device, unless:

(1) A student initiates a video chat or audio chat with the school-based personnel or 1-to-1 device provider;

(2) The activation and access is ordered pursuant to a judicial warrant; or

(3)(A) Doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose; and

(B) Within 72 hours of accessing a 1-to-1 device's audio or video receiving, transmitting, or recording functions are accessed in response to an imminent threat to life or safety, the school-based personnel or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data and features were accessed.

(e) No school-based personnel may use a 1-to-1 device, or require a student to use a 1-to-1 device in their presence, in order to view or gain access to a student's password protected software, online accounts or applications, except where:

(1) The school-based personnel is a teacher;

(2) The student is enrolled in and participating in a class taught by the teacher; and

(3) The viewing of the password protected software, online accounts, or applications relates exclusively to an educational purpose.

(f) A 1-to-1 device provider shall not use any student data or personally identifiable student information stored on or retrieved from a 1-to-1 device to:

(1) Inform, influence, or direct marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement as outlined in section 6 of this act; or

(2) Develop, in full or in part, a student profile for any commercial or other non-educational purpose.

(g) Notwithstanding any other provisions in this section, school-based personnel may not supervise, direct, or participate in a 1-to-1 program, or access any 1-to-1 device or data thereupon, until he or she has received training to ensure the employee's understanding and compliance with the provisions of this section.

(h)(1) No personally identifiable student information obtained or received from a 1-to-1 device by school-based personnel or 1-to-1 device provider may be sold, shared, or otherwise transferred to another person or entity, except:

(A) To another school employee who has satisfied the requirements of subsection (g) of this section and is accessing the information in furtherance of the employee's professional duties;

(B) Where a 1-to-1 device provider has been authorized to do so pursuant to an opt-in agreement; or

(C)(1) In the case of a 1-to-1 device provider, such information is sold as part of a sale or merger of the entirety of the 1-to-1 device provider's business.

(2) Any entity that receives personally identifiable student information shall be subject to the same restrictions and obligations under this section as the 1-to-1 device provider from which the personally identifiable student information was obtained.

(i) No person or entity, other than an educational institution, school-based personnel, 1-to-1 device provider, or the student's parent or legal guardian subject to the limitations set forth in this section, shall be provided direct access to review or interact with a 1-to-1 device and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or upon the express permission of the student to whom the 1-to-1 device is issued.

(j) When a 1-to-1 device is permanently returned by a student, the educational institution or 1-to-1 device provider who provided it shall, without otherwise accessing the data on the 1-to-1 device, fully erase all the data stored on the device and return the device to its default factory settings.

Sec. 5. Opt-in agreements for 1-to-1 devices and programs.

(a) A valid opt-in agreement shall identify, with specificity:

(1) A description of the specific personally identifiable student information on the 1-to-1 device that will be accessed, analyzed, or interacted with;

(2) The name of the school-based personnel or 1-to-1 device provider to whom the authority to access, analyze, and interact with the personally identifiable student information on the 1-to-1 device is being granted;

(3) The educational purpose(s) for which the school-based personnel or 1-to-1 device provider is being granted the authority to access, analyze and interact with the personally identifiable student information on the 1-to-1 device; and

(4) The individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall only be valid if it has been signed by:

(1) The student's parent or legal guardian, if the student is in elementary school;

(2) The student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(3) The student alone, if the student has reached the age of majority.

(c) An opt-in agreement shall not be valid if it actually or effectively grants a 1-to-1 device provider:

(1) General authority to access a student's 1-to-1 device; or

(2) The authority to collect all the personally identifiable student information that is generated by or used in connection with a specific program or application.

(d) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person(s) eligible to authorize an opt-in agreement pursuant to subsection (b). Within 30 days of such a revocation, notice to any affected third parties shall be made by the educational institution.

(e) A 1-to-1 device provider that accesses, analyzes, or interacts with personally identifiable student information on a 1-to-1 device shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(f) No 1-to-1 device program offered to an educational institution or its students may be conditioned upon the exclusive use of any software, application, website or Internet-based service sold or provided by the 1-to-1 device provider.

(g) No 1-to-1 device or related educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian:

(1) Based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement; or

(2) Based in whole or in part upon a student's refusal to open, close, or maintain an email or other electronic communications or social media account with a specific service provider.

(h) A 1-to-1 device provider shall violate section 4(g)(1) if it conditions the offer, provision or receipt of a 1-to-1 device upon a student's or the student's parent's or legal guardian's agreement to provide access to personally identifiable student information.

Sec. 6. Student user name and password privacy.

(a) An educational institution shall not:

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

(2) Require, request, or coerce a student or prospective student to access a personal social media account in the presence of school-based personnel or school volunteer, including, but not limited to, a coach, teacher, or school administer, in a manner that enables the school-based personnel or school volunteer to observe the contents of such account;

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

(b) An educational institution shall not take any action or threaten to take any action to discipline, expel, unenroll, prohibit from participating in curricular or extracurricular activities,

or otherwise penalize a student for a student's refusal to disclose any information or perform acts as specified in paragraph (a) of this section.

(c) A prospective student's refusal to disclose any information or perform acts as specified in paragraph (a) of this section shall not be cause to refuse the prospective student admission to a school.

(d) Nothing in this act shall prevent an educational institution from:

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

(2) Complying with District 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 user name and password, password, or other means of authentication that provides access to a personal social media account, for the purpose of:

(A) Ensuring compliance with applicable laws or regulatory requirements; or

(B) Investigating an allegation, based on receipt of specific information, of unlawful harassment or bullying of another 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.

(e) If an educational institution inadvertently receives the user name and 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 educational institution's network or educational institution-provided devices, the educational institution is not liable for having the information, but may not use the information to access the personal social media account of the student or prospective student, may not share the information with anyone, and must delete the information immediately or as soon as is reasonably practicable.

Sec. 7. Student's personal electronic devices on campus.

(a) School-based personnel may not access, or compel a student to produce, display, share or provide access to, any data or other content input into, stored upon, or accessible from a student's personal technological device, even where the personal technological device is being carried or used in violation of an educational institution policy.

(b) Notwithstanding paragraph (a) of this section, school-based personnel may search a student's personal technological device, if:

(1) The school-based personnel has a reasonable suspicion that a student has violated or is violating an educational institution policy and that the student's personal technological device contains evidence of the suspected violation. In such cases, school-based personnel may search the student's personal technological device if:

(A) The student's personal technological device is located on the property of the educational institution;

(B) Prior to searching a student's personal technological device, the school-based personnel:

(i) Documents the reasonable suspicion giving rise to the need for the search; and

(ii) Notifies the student and the student's parent or legal guardian of the suspected violation and what data will be accessed in searching for evidence of the violation.

(2) The search is strictly limited to components of the device or data on the device reasonably likely to yield evidence of the suspected policy violation. No person shall be permitted to copy, share, or transfer any data or any information obtained pursuant to a search under this subsection that is unrelated to the suspected violation that prompted the search;

(3)(A) Doing so is necessary in response to an imminent threat to life or safety.

(B) Within 72 hours of accessing a personal technological device in response to an imminent threat to life or safety, the school-based personnel or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data was accessed.

(c) Pursuant to paragraph (a) of this section, an educational institution, subject to any other relevant legal restrictions, may seize a student's personal technological device to prevent data deletion pending notification, provided that:

(1) The pre-notification seizure period is no greater than 48 hours; and

(2) The personal technological device is stored securely on educational institution property and not accessed during the pre-notification seizure period.

(d) Notwithstanding paragraph (a) of this section, where a student is suspected of illegal conduct, no search of the student's personal technological device may occur unless a judicial

warrant authorizing a law enforcement official to search the student's personal electronic device has been secured, even if the student is also suspected of a related or unrelated violation of an educational institution policy.

Sec. 8. Limitation on use.

(a) Evidence or information obtained or collected in violation of this act shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.

Sec. 9. Enforcement and rules.

(a) OSSE is empowered to carry out and enforce the provisions of this act. Within 90 days of the effective date of this act, OSSE shall promulgate such rules or regulations as may be necessary to effectuate the purposes of this act.

(b) Any individual who claims that a violation of this act has injured his or her personal reputation may bring a civil action against the educational institution or 1-to-1 device provider before a court or a jury in the Superior Court of the District of Columbia seeking equitable relief and damages, including, compensatory damages for mental pain and suffering and reasonable costs and attorneys' fees. A civil action instituted pursuant to this section shall be filed within 3 years of the violation or within one year of the individual gaining knowledge of the violation, whichever occurs first. D.C. Official Code § 12-309 shall not apply to any civil action brought under this section.

(c) Any school-based personnel who violates this act, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For school employees who are represented under the terms of a collective bargaining agreement, this act prevails except where it conflicts with the collective bargaining agreement, any memorandum of

agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

Sec. 10. Fiscal impact statement.

The Council adopts the fiscal impact statement [in the committee report][of the Budget Director][of the Chief Financial Officer] as the fiscal impact statement required by section 4a of the General Legislative Procedures Act of 1975, approved October 16, 2006 (120 Stat. 2038; D.C. Official Code § 1-301.47a).

Sec. 11. Effective date.

This act shall take effect following approval by the Mayor (or in the event of veto by the Mayor, action by Council to override the veto), a 30-day period of congressional review as provided in section 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(1)), and publication in the District of Columbia Register.