HOUSE DOCKET, NO. 3347 FILED ON: 2/19/2021

HOUSE . . . . . No. 107

The Commonwealth of Massachusetts

PRESENTED BY:

Patricia A. Duffy

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act regulating privacy and technology in education.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
Patricia A. Duffy	*5th Hampden*	*2/19/2021*
Kirstin Beatty	*149 Central Park Drive, Holyoke, MA 01040*	*2/19/2021*

HOUSE DOCKET, NO. 3347 FILED ON: 2/19/2021

HOUSE . . . . . No. 107

By Ms. Duffy of Holyoke, a petition (accompanied by bill, House, No. 107) of Patricia A. Duffy and Kirstin Beatty regulating privacy and technology in education. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

An Act regulating privacy and technology in education.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The legislature finds and declares all of the following:

Whereas, data collection is taking center stage in education as part of ongoing "accountability" and "personalized learning" - a surveillance industry.

Whereas, surveillance and intense data collection disrupts relationship-building between children, youth, and mentors, and the use of that data to manipulate and influence behavior is abhorrent.

Whereas, community opposition prevented St. Paul school districts from sharing markers such as welfare, grades and suspensions with the city to flag children for future involvement with juvenile justice.

Whereas, Massachusetts schools collect confidential data, including unintentionally through educational software use, and including biometric data such as to recognize fingerprint, voice, and typing.

Whereas, Massachusetts has earned an F for its privacy laws from the Parent Coalition for Student Privacy.

Whereas, no one can promise full protection of confidential data, even if anonymized, and ransomware attacks are common.

Whereas, surveillance and confidential data capture raises Orwellian questions and risks of criminal misuse.

Whereas, school evaluation data, testing, and standardization proofs are subtracting significantly from positive school cultures and time on learning.

SECTION 2. Chapter 69 of the General Laws is hereby amended by adding the following section:--

Section 1R. (a) Definitions. As used in this section, the following words shall have the following meanings:

“Authority” is the authority legally invested with setting policy for a public charter school, virtual school, or, in the case of a school district, the elected school committee.

“Board" is the board of elementary and secondary education.

"Commissioner" is the commissioner of elementary and secondary education.

"Department" is the department of elementary and secondary education.

"Information technology" is the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

"Screen time" is time viewing a technological or digital screen which includes but is not limited to a television, a smart board, projector, or computer.

"Confidential data" is data collected on students or staff and which includes:

(1) standard identifying information:

i. names of staff and students

ii. dates of birth

iii. addresses

iv. grades

v. medical information

vi. exam results

vii. staff development reviews

viii. assessments

ix. other personal identifying information

(2) identifying data such as location-tracking, photographs, and biometric data, which includes unique biological or behavioral identifiers such but not limited to voice audio, fingerprints, gait recognition, and keystroke dynamics.

(3) personal writings or other personal work such as art

(4) political views

(5) socioeconomic data

(6) disciplinary data

(7) similar data or information on other individuals that are not students or staff, but may be referenced in or extracted from student and staff data.

(8) observed and inferred data from the data provided

(b) End technology mandate across curriculum. The board, commissioner, and department shall revise state education goals, curriculum frameworks, and evaluation requirements to require use of digital and information technology only in extracurricular courses in the subject area, and to eliminate any other mandate for the use of digital or information technology across the curriculum in all subjects in regards to state education goals, curriculum frameworks, and student, teacher, and school evaluation.

(c) Policy directives. The commissioner, board, and department shall enact and enforce the following policy directives wherever possible, and shall in no way limit the ability of public schools and school districts to set rules or policy that are more stringent than here listed.

(1) Less tech. Prefer and support the use of less information technology in all arenas of public education, including, but not limited to student education, administration, data management, teacher training and evaluation, building management, and school evaluation, including as follows:

(i) When educational benefits are equal between use of or non-use of information technology, choose non-use of information technology.

(ii) When non-use of technology would result in disruption of a data system, then evaluate whether the data system can be successfully replaced with one that does not use digital or information technology.

(iii) Periodically reevaluate if less information technology can be utilized to achieve the educational purpose.

(iv) Provide for support and professional development to encourage non-use of technology in education.

(v) Encourage students, teachers, and school staff or administrators to use printed or cursive text rather than word processing and offline filing systems.

(2) Less data. Reduce and limit collection of confidential data in all arenas of public education including, but not limited to, as follows:

(i) Require all data collection serve a predetermined, specific educational purpose that benefits the students from whom the data is collected.

(ii) Prohibit and, if existing, halt collection of biometric data – if biometric data is collected within a public school for medical purposes, then require data be destroyed following medical use, not be repurposed, or condition further use on fully informed consent of the patient or patient's guardian freely granted.

(iii) Substantially reduce the amount of confidential data gathered and used for data analytics by setting fewer confidential data points for collection, such as with regards to the evaluation of teachers, students, and schools.

(iv) When data collection is required by state or federal law, where possible prefer to emphasize non-confidential data points instead of confidential data – non-confidential data points may include but not be limited to school air quality, building condition, and length of recess periods.

(v) Discourage the evaluation of schools, student and school staff using information technology, and instead prefer offline, real-life evaluations.

(vi) Provide that excessive use of data analytics and excessive testing for data analytics both be a negative factor in formal evaluation of schools.

(vii) When using digital technology, limit infringement of privacy by opting for the least intrusive digital technology to serve the educational purpose.

(viii) Limit use of digital voice, video calls, and online proctoring, and when using justify this level of confidential data collection is necessary to serve the educational purpose, and cannot otherwise be addressed. If using online voice, video, and proctoring, record in writing the reasons why this is necessary in specific cases.

(ix) Require school-wide policies on how to handle video footage in connection with online voice and video calls, including at a minimum agreements on (A) showing students and staff on screen and making recordings; (B) informing the subjects about the data, e.g. retention

period and period of recordings; (C) if applicable, secure storage and who is responsible for deletion.

(x) Set institutional and school-wide policies on remote testing.

(xi) Significantly restrict use of information technology by students in elementary education.

(xii) Insure digital data that is no longer needed is destroyed.

(xii) Provide training and set policies for students and staff regarding the use of digital technology to minimize data collection.

(xiii) When transfer of school evaluation data is necessary, insure data transfer does not involve data tied to individuals and which can be reassembled by artificial intelligence and tied to individual profiles – instead, insure data analysis and aggregation occurred previous to transfer and is formatted to prevent deanonymization.

(3) Rights. Respect rights to privacy, to transparent government institutions, to health, and to informed consent or dissent in all arenas of education, including, but not limited to, as follows:

(i) Provide students, guardians, and staff in easy-to-understand language information specific to each digital product or digital service regarding the confidential data collected, purposes to which the information will be used, the security practices in place, algorithms behind decision making, parties to the confidential data, legal contact information for those parties,

procedures for deleting the confidential data, and any attendant risks provided in the product manual or service contract or otherwise known to exist regarding the product or service.

(ii) Disclose collection of confidential data to staff and student guardians, and if of age, students. Except with regards to data collection required for operations and to which the educational institution's interest outweighs the student's, condition confidential data collection on fully informed consent.

(ii) For students who successfully object to data collection, offer a suitable alternative that sufficiently addresses their privacy concerns. This alternative should not entail any adverse consequences such as disproportionate delay to the student's progress.

(iii) For staff who successfully object to data collection, there should be no adverse consequences.

(iii) Set up a process to allow students and guardians to access confidential data.

(iv) When considering use of surveillance, require proof that less intrusive means would not suffice.

(v) Prevent and discourage the routine surveillance of students and school staff in classrooms or through digital school assignments and assigned technologies, excepting surveillance outside the building to prevent vandalism and burglary where reasonably warranted.

(vi) Prohibit and discourage the use of RFID and other technologies to track staff and students, except where an individualized education plan requires for student safety.

(vii) Require a police warrant for temporary surveillance cameras when criminal concerns arise.

(viii) Prohibit and discourage administrative monitoring or checking of private, external student and school staff internet use and social media accounts without a legitimate safety concern and without a warrant.

(ix) Prohibit the use of predictive analytical software regarding student and staff behaviors and futures, including sharing of such data or profiles with third parties.

(x) When technology is used, insure products, software, installation and usage reflects the best cautionary practices for safer and healthier technology with respect to chemical, neurological, and electromagnetic concerns, posture, movement, eye rest, digital addiction, and screen light.

(xi) Educational research requires the fully-informed consent of guardians and, if of age, students, and may not be offered in exchange for educational services or other benefits to the students.

(xii) Prohibit the taking of educator and student intellectual property by the school authority, school administration or other supervisors, other educators, and third parties such as software companies or researchers.

(xiii) Through policy, inventory, and education, prevent idle capturing of biometric or confidential data through personal and institutional digital devices, whether cellphones, laptops, or other devices.

(4) Cybersecurity. Secure existing data including, but not limited to, as follows.

(i) Limit travel and sharing of student and staff confidential data where possible, for example preferring to keep student data with the student, classroom data with the teacher, and school data housed with the school.

(ii) Prefer to publish confidential data in private, closed networks or on paper offline. Prefer printed text or hard-wired, offline closed systems for confidential data storage.

(iii) Routinely check cybersecurity and harden systems in use.

(iv) At minimum, provide encryption of personal data at motion and at rest, required training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor. Passwords should be protected in the same manner as all other personal student information.

(v) Insure that there are data protection resource personnel to equitably assist educators to prevent the loss of confidential data while using digital technology.

(vi) Subdivide confidential into different data storage locations to limit damage if lost or stolen.

(5) Procurement. Procure software and set data processing agreements which protect students and staff, including, but not limited to, as follows:

(i) Identify and limit use of products, companies, or consultants with a history of disregarding privacy protections or with poor cybersecurity - decommission software and equipment which pose such risks.

(ii) Identify and discourage or prohibit use of new technologies and practices which threaten privacy and cybersecurity of school students, staff, and the department.

(iii) Select a software supplier, broadband provider, and digital technologies that comply with local, state, and federal laws and this policy.

(iv) Set a data processing agreement in place that protects students and staff which, at a minimum, includes the following requirements:

(A) Comply with the privacy and security intentions of this section.

(B) Insure that when digital technologies are utilized for which third parties such as software companies have access to data, only the minimum of student and staff data necessary to complete a specified, predetermined educational purpose is available to the third party, only the minimum of data necessary is retained only as long as is needed, and that data is not further shared and is not used for purposes other than as contracted.

(C) Insure data and profiles are utilized only for specified, predetermined educational purposes, and are not repurposed without express, fully informed student and guardian consent moderated through the school authority.

(D) Provide prompt notification in event of any breach of security, as well as evidence of insurance coverage for any breach.

(E) Provide in accessible, easy-to-understand language a fact sheet of information specific to each digital product or service regarding the confidential data collected, purposes to which the information will be used, the security practices in place, algorithms behind decision making, parties to the confidential data, legal contact information for those parties, procedures for reviewing or deleting confidential data, and any attendant risks provided in the product manual or service contract or otherwise known to exist regarding the digital product or service.

(F) Once the specified, predetermined educational purpose is accomplished and the confidential data is no longer required, destroy the confidential data.

(G) Prohibit the sharing of confidential data, limiting confidential data to remain available only for its predetermined, specific educational use to the minimum persons and artificial intelligence necessary to accomplish that use – no re-disclosures to additional individuals, subcontractors, affiliates, parent companies, or organizations.

(H) Prohibit the taking of educator and student intellectual property.

(I) Provide a process for guardians or students to review confidential data collected, delete if in error or nonessential to the student's transcript, and to opt out of further collection unless that data is part of the student's educational records.

SECTION 2. Section 1I of chapter 69 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by inserting after the second sentence the following:-

In addition, the system shall assess relevant institutional circumstances and responsibilities including building and environmental health conditions; provisions for age-appropriate work breaks and recess; accommodations for academic freedom and academic flexibility; compliance with limits on screen time; provisions for student and staff safety during and after school hours; and protections for cybersecurity and privacy.

SECTION 3. Section 1I of chapter 69 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking the second paragraph and inserting in place the following:-

The system shall be designed both to measure outcomes and results regarding student performance and serve to assist student and public school improvement. In its design and application, the system shall strike a balance among considerations of accuracy, fairness, expense and administration, and shall also protect privacy, academic biodiversity, and time on learning, in particular with regard to students and teachers.

In accordance with section 1R, the system shall be designed to protect the privacy of students, staff, and administration. Therefore, the board, department, and commissioner shall be tasked with designing systems which limit confidential data collection and transfer and, where data transferred is confidential, rely on paper or otherwise revise collection requirements to prevent digital collection and digital transfer of confidential data. The board, department, and commissioner shall seek not only to minimize all such digital data collection, but to design a system that limits the intrusion of data collection upon learning, including but not limited to demands on time and money.

Where questions remain regarding the efficacy or review of any school, the board shall rely on a formal visitation and review, but shall insure such a review is dominated by former and existing Massachusetts public school teachers and a minority of public school administrators. In the case of students whose performance is difficult to assess using conventional methods, the board may require consideration of work samples, projects and portfolios.

SECTION 4. Section 1I of chapter 69 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking the sentence “All information filed pursuant to this section shall be filed in the manner and form prescribed by the department.” and inserting in place the following:-

All information filed pursuant to this section shall be filed in the manner and form prescribed by the department, provided such filing conforms to section 1R.

SECTION 5. Section 1I of chapter 69 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking the seventh paragraph and inserting in place the following:-

Each school district shall maintain individual records on every student and employee in accordance with section 1R. Each student record shall contain a unique and confidential identification number, basic demographic information, program and course information. Each employee record shall include a unique and confidential identification number, basic demographic information, relevant certification, relevant academic credits, program and course information, and relevant disciplinary and evaluation records.

SECTION 6. Section 1I of chapter 69 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking the sentence “Each school district and charter school shall furnish in a timely manner such additional information as the department shall request,” and inserting in place the following:-

Each school district and charter school shall furnish in a timely manner such additional information as the department may reasonably request, while the department shall insure such requests are not only reasonable, but that submission requirements comply with section 1R.

SECTION 7. Subsection (l) of Section 94 of Chapter 71 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking out paragraph (13) and replacing with:--

(13) provisions for cybersecurity, privacy, cyber-safety, data processing agreements, and safer technology;

SECTION 8. Subsection (b) of Section 94 of Chapter 71 of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by adding after the third sentence the following:

In evaluating whether to allow continued certification, the board shall require the virtual school has evidence of serving as a benefit to the overarching public education system, of compliance with this section and state laws, of reasonable spending, and of attention and benefits to student education, including but not limited to the following considerations:

(1) whether the virtual school has appropriately entered into data processing agreements with third party software and internet providers and taken other steps to comply with state and federal data protection laws;

(2) whether the virtual school has chosen trustworthy partners for third party software and internet providers;

(3) whether the virtual school assures the student a safe space to work and, if relevant, provides for safe and secure technology;

(4) whether the virtual school demonstrates restraint in spending tax monies, with salaries and funds for administration and staff per pupil comparable to brick-and-mortar public schools or otherwise justifiable;

(5) whether there is evidence the social and emotional health of students attending the virtual school is worse as a result of attending the school, and if so, whether this is due to an aspect of the program, of the student, or both.

(6) whether the virtual school has taken reasonable measures, where possible, to reduce time spent before digital screens.

(7) whether the virtual school insures easy access weekly to an appropriately certified teacher in the classroom subject areas through virtual, real-time office hours.

(8) whether the virtual school insures virtual, real-time access to and lessons from an appropriately certified and unscripted teacher for some, if not all, classroom lessons as a matter of routine, rather than relying on automated or AI systems for instruction.

SECTION 9. Clause (b) of Section 7A of Chapter 15A of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking out the “and (9) maximizing fundraising for private sources” and inserting in place thereof the following clauses: --

(9) maximizing fundraising from private sources with transparency; (10) maximizing safety, security, and privacy of digital and communications technology; and (11) protecting academic currency, diversity, and freedom against political, industrial, and technological control.

SECTION 10. Section 7A (1) of Chapter 15A of the General Laws, as appearing in the 2021 Official Edition, is hereby amended by striking out the “and (9) maximizing fundraising for private sources.” and inserting in place thereof the following clauses: --

(9) maximizing fundraising from private sources with transparency; (10) maximizing safety, security, and privacy of digital and communications technology; and (11) protecting academic currency, diversity, and freedom against political, industrial, and technological control.

SECTION 11. Chapter 15A of the General Laws is hereby amended by adding the following section:--

Regulated tech in higher education.

(a) Definitions.

"Confidential data" is data collected on students or staff and which includes:

(1) standard identifying information:

i. names of staff and students

ii. dates of birth

iii. addresses

iv. grades

v. medical information

vi. exam results

vii. staff development reviews

viii. assessments

ix. other personal identifying information

(2) identifying data such as location-tracking, photographs, and biometric data, which includes unique biological or behavioral identifiers such but not limited to voice audio, fingerprints, gait recognition, and keystroke dynamics.

(3) personal writings or other personal work such as art

(4) political views

(5) socioeconomic data

(6) disciplinary data

(7) similar data or information on other individuals that are not students or staff, but may be referenced in or extracted from student and staff data.

(8) observed and inferred data from the data provided

"Staff" refers to all staff, including but not limited to professors, administrators, groundskeepers, cafeteria workers, and others at institutions of higher education within the Commonwealth.

(b) Higher education 5-year plan and mission. Following the procedures of section 7 of this Chapter, the council, board of trustees, and secretary shall revise educational missions and 5-year plans to promote privacy rights, safer technology, and to protect educational autonomy and academic freedom in the public interest over mass instruction, as well as to reduce dependence on technology and for safer, regulated use of information technology by students and staff at public institutions of higher education. The secretary shall provide an annual public report and presentation to the legislative committee(s) charged with higher education on progress, obstacles,

and changes in relation to the intent of this section, including with regard to safer, regulated technology as described in subsection (e).

(d) Accountability and evaluation. With respect to section 7A of this Chapter and following the procedures therein, the board of higher education shall revise accountability and evaluation standards to protect privacy rights, promote safer technology, and to protect educational autonomy and academic freedom over mass instruction along with a focus on reducing dependence on technology and for regulated, safer use of technology by students and staff at public institutions of higher education. Incorporated into accountability standards shall be those listed in subsection (e).

(e) The council, secretary, and board of trustees shall be responsible for insuring the adoption of stringent measures to protect student and staff confidential data and safer use of technology, including as follows:

(1) Less tech. Prefer and support the use of less information technology where possible:

(i) When educational benefits are equal between use of or non-use of information technology, choose non-use of information technology.

(ii) When non-use of technology would result in disruption of a data system, then evaluate whether the data system can be successfully replaced with one that does not use digital or information technology.

(iii) Periodically reevaluate if less information technology can be utilized to achieve the educational purpose.

(iv) Provide for support and professional development to encourage non-use of technology in education.

(v) Encourage students and staff to use printed or cursive text when suitable and to limit use of information technology for word processing.

(2) Less data. Reduce and limit collection of confidential data including, but not limited to, as follows:

(i) Require all data collection serve a predetermined, specific educational purpose that benefits the students from whom the data is collected.

(ii) Prohibit and, if existing, halt collection of biometric data – if biometric data is collected within a public school for medical purposes, then require data be destroyed following medical use, not be repurposed, or condition further use on fully informed consent of the patient or patient's guardian freely granted.

(iii) Substantially reduce the amount of confidential data gathered and used for data analytics by setting fewer confidential data points for collection, such as with regards to the evaluation.

(iv) When data collection is required by state or federal law, where possible prefer to emphasize non-confidential data points instead of confidential data.

(v) Discourage evaluation or proctoring using information technology, and instead prefer offline, real-life evaluations and proctoring.

(vi) When using digital technology, limit infringement of privacy by opting for the least intrusive digital technology to serve the educational purpose.

(vii) Require institutional policies on how to handle video footage in connection with online voice and video calls, including at a minimum agreements on (A) showing students and staff on screen and making recordings; (B) informing the subjects about the data, e.g. retention period and period of recordings; (C) if applicable, secure storage and who is responsible for deletion.

(viii) Set institutional and school-wide policies on remote testing.

(ix) Insure digital data that is no longer needed is destroyed.

(x) Provide training and set policies for students and staff regarding the use of digital technology in order to minimize data collection.

(xi) When transfer of institutional data is necessary, insure data transfer does not involve data tied to individuals and which can be reassembled by artificial intelligence and tied to individual profiles – instead, insure data analysis and aggregation occurred previous to transfer and is formatted to prevent deanonymization.

(3) Rights. Respect rights to privacy, to transparent government institutions, to health, and to informed consent or dissent in all arenas of education, including, but not limited to, as follows:

(i) To staff and students provide, in easy-to-understand language, information specific to each digital product or digital service regarding the confidential data collected, purposes to which the information will be used, the security practices in place, algorithms behind decision making, parties to the confidential data, legal contact information for those parties, procedures

for deleting the confidential data, and any attendant risks provided in the product manual or service contract or otherwise known to exist regarding the product or service.

(ii) Disclose collection of confidential data to staff and students. Except with regards to data collection required for higher education operations and to which the institutional interest outweighs, condition confidential data collection on fully informed consent.

(iii) For students who successfully object to data collection, offer a suitable alternative that sufficiently addresses their privacy concerns. This alternative should not entail any adverse consequences such as disproportionate delay to the student's progress.

(iv) For staff who successfully object to data collection, there should be no adverse consequences.

(vi) Set up a process to allow students and guardians to access confidential data.

(vii) When considering use of surveillance, require proof that less intrusive means would not suffice.

(viii) Prevent and discourage the routine surveillance of students and staff in classrooms or through digital school assignments and assigned technologies, excepting surveillance outside the building to prevent vandalism and burglary where reasonably warranted.

(vi) Prohibit and discourage the use of RFID and other technologies to track staff and students, except where required for disability.

(vii) Require a police warrant for temporary surveillance cameras when criminal concerns arise.

(viii) Prohibit and discourage administrative monitoring or checking of private, external student and school staff internet use and social media accounts without a legitimate safety concern and without a warrant.

(ix) Prohibit the use of predictive analytical software regarding student and staff behaviors and futures, including sharing of such data or profiles with third parties.

(x) When technology is used, insure products, software, installation and usage reflects the best cautionary practices for safer and healthier technology with respect to chemical, neurological, and electromagnetic concerns, posture, movement, eye rest, digital addiction, and screen light.

(xi) Educational research requires the fully-informed consent of guardians and, if of age, students, and may not be offered in exchange for educational services or other benefits to the students.

(xii) Prohibit the taking of educator and student intellectual property by administration, supervisors, other educators, and third parties such as software companies or researchers.

(xiii) Through policy, inventory, and education, prevent idle capturing of biometric or confidential data through personal and institutional digital devices, whether cellphones, laptops, or other devices.

(4) Cybersecurity. Secure existing data including, but not limited to, as follows.

(i) Limit travel and sharing of student and staff confidential data where possible, for example preferring to keep student data with the student, classroom data with the teacher, and school data housed with the school.

(ii) Prefer to publish confidential data in private, closed networks or on paper offline. Prefer printed text or hard-wired, offline closed systems for confidential data storage.

(iii) Routinely check cybersecurity and harden systems in use.

(iv) At minimum, provide encryption of personal data at motion and at rest, required training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor. Passwords should be protected in the same manner as all other personal student information.

(v) Insure that there are data protection resource personnel to equitably assist educators to prevent the loss of confidential data while using digital technology.

(vi) Subdivide confidential data into different storage locations to limit damage if lost or stolen.

(5) Procurement. Procure software and set data processing agreements which protect students and staff, including, but not limited to, as follows:

(i) Identify and limit use of products, companies, or consultants with a history of disregarding privacy protections or with poor cybersecurity - decommission software and equipment which pose such risks.

(ii) Identify and discourage or prohibit use of new technologies and practices which threaten privacy and cybersecurity of students, staff, and the department.

(iii) Select a software supplier, broadband provider, and digital technologies that comply with local, state, and federal laws and this section.

(iv) Set a data processing agreement in place that protects students and staff which, at a minimum, includes the following requirements:

(A) Comply with the privacy and security intentions of this section.

(B) Insure that when digital technologies are utilized for which third parties such as software companies have access to data, only the minimum of student and staff data necessary to complete a specified, predetermined educational purpose is available to the third party, only the minimum of data necessary is retained only as long as is needed, and that data is not further shared and is not used for purposes other than as contracted.

(C) Insure data and profiles are utilized only for specified, predetermined educational purposes, and are not repurposed without express, fully informed student consent moderated through the educational institution.

(D) Provide prompt notification in event of any breach of security, as well as evidence of insurance coverage to cover any breach.

(E) Provide in accessible, easy-to-understand language a fact sheet of information specific to each digital product or service regarding the confidential data collected, purposes to which the information will be used, the security practices in place, algorithms behind decision making, parties to the confidential data, legal contact information for those parties, procedures for reviewing or deleting confidential data, and any attendant risks provided in the product manual or service contract or otherwise known to exist regarding the digital product or service.

(F) Once the specified, predetermined educational purpose is accomplished and the confidential data is no longer required, destroy the confidential data.

(G) Prohibit the sharing of confidential data, limiting confidential data to remain available only for its predetermined, specific educational use to the minimum persons and artificial intelligence necessary to accomplish that use – no re-disclosures to additional individuals, subcontractors, affiliates, parent companies, or organizations.

(H) Prohibit the taking of educator and student intellectual property.

(I) Provide a process for students to review confidential data collected, delete if in error or nonessential to the student's transcript, and to opt out of further collection unless that data is part of the student's educational records.