Cambridge Public Schools
Comprehensive Written Information Security Plan

I. Objective

The objective of the Cambridge Public Schools is to create effective, administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts and to comply with its obligations under 201 C.M.R. 17.00. This plan sets forth the procedure for evaluating the Cambridge Public Schools' electronic and physical methods of accessing, collecting, storing, using, disseminating, transmitting, storing, retaining, protecting and destroying personal and/or student record information of residents of the Commonwealth, whether stored electronically, in paper or in another format, including without limitation, when used or released in connection with any research projects[1] involving student data, including without limitation, student record information.

II. Definitions

A. Personal Information. For purposes of this plan, "Personal Information" is defined as a Massachusetts resident's first and last name or the first initial and last name in combination with any one of the following pieces of information that relate to such resident:

a. social security number;

b. driver's license number or state-issued identification card number; or

c. financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account.

"Personal information" shall not include information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.

B. Student Record Information. For purposes of this plan, "Student Record Information" is defined as all information in the student record, including the transcript and the temporary record, including all information, recordings and computer tapes, microfilm, microfiche or any other materials regardless of physical form or characteristics concerning a student that is organized on the basis of the student's name or

[1] Please note that all research projects must be first be approved by the Deputy Superintendent for Teaching & Learning.

in a way that such student may be individually identified, and that is kept by the public schools of the Commonwealth, regardless of where the materials are located. Such information is of importance to the educational process and may include, but is not limited to, standardized test results, class rank, extracurricular activities and evaluations by teachers, counselors, and other school staff.

III. Purposes:

The purposes of this plan are to:

a. Ensure the security and confidentiality of personal information and student record information;

b. Protect against any anticipated threats or hazards to the security or integrity of such information; and

c. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents and/or improper use of such information.

IV. Scope

In formulating and implementing the plan, the Cambridge Public Schools will do the following:

a. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal and/or student record information;

b. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal and/or student record information;

c. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards to control such risks;

d. Design and implement a program that puts safeguards in place to minimize those risks, consistent with the requirements of 201 C.M.R. 17.00 and federal and state student record regulations; and

e. Regularly monitor the effectiveness of those safeguards.

V. Data Security Coordinator

The Cambridge Public Schools has designated the Chief Information Officer to implement, supervise, and maintain the program and as such is deemed to be the "Data Security Coordinator." The Data Security Coordinator will be responsible for:

(a) Initial implementation of the program;

(b) Training staff on the program;

(c) Regularly testing the program's safeguards;

(d) Evaluating the ability of third party service providers to protect personal information collected that the Cambridge Public Schools has permitted the third party providers to access.

(e) Reviewing the scope of the security measures in the program at least annually or whenever there is a material change in the practices of the office that may implicate the security or integrity of records containing personal information and/or student record information

VI. Internal Risks

The following measures are mandatory and effective immediately in order to combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information and/or student record information, and evaluating and improving the effectiveness of the current safeguards.

a. The amount of information collected must be limited to that amount reasonably necessary to accomplish the legitimate business purposes, or necessary for compliance with state and federal laws and regulations.

b. Access to records containing personal information and/or student record information shall be limited to those persons who are reasonably required to know the information in order to accomplish legitimate business/educational purposes in connection with their duties or to enable the Cambridge Public Schools to comply with federal and state law and regulations.

c. All files containing personal information and/or student record information shall be stored securely in locked facilities, storage areas or containers to protect the information against unauthorized access, destruction, use, modification, disclosure or loss and all files containing personal information shall be destroyed as soon as

the information is no longer needed or required to be maintained by state or federal record retention requirements in accordance with appropriate destruction methods as designated by the Chief Information Officer.

d. All security measures should be reviewed annually or when there is a material change in the business practices of the office that may reasonably implicate the security or integrity of records containing personal information and/or student record information.

e. Paper or electronic records, including records stored on hard drives or other electronic media containing personal information shall be disposed of only in a manner that complies with M.G.L. c. 93I, and paper or electronic records, including records stored on hard drives or other electronic media containing student record information shall be disposed on in a manner that complies with federal and state student record regulations and M.G.L.c. 93I.

f. Employees are encouraged to report any suspicious or unauthorized use of personal information and/or student record information.

g. Whenever there is a security breach the Chief Information Officer shall be notified so that a determination can be made as to whether there was a security breach that requires notification under M.G.L., c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes to the security practices are required to improve the security of personal information and/or student record information for which the office is responsible.

h. Access to electronically stored personal information and/or student record information shall be electronically limited to those employees having a unique log in ID; and re-log-in shall be required when a computer has been inactive for thirty (30) minutes or more.

i. Employees are prohibited from keeping open files containing personal information and/or student record information on their desks when they are not at their desks.

j. At the end of the work day, all files and other records containing personal information and/or student record information must be secured in a manner that is consistent with the plan's rules for protecting the security of personal information and/or student record information.

k. Terminated or temporary employees must return all records containing personal information and/or student record information, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

l. A terminated or temporary employee's physical and electronic access to personal information and/or student record information must be immediately blocked. Such terminated employees shall be required to surrender all keys and access codes that permit access to the office or information. The terminated or temporary employee's remote electronic access to personal information and/or student record information must be disabled; their voicemail access, Internet access, email access, and passwords must be invalidated.

m. Current employees user-ID's and passwords must be changed at least every six (6) months.

n. Employees are prohibited from transmitting or storing records containing personal information and/or student record information on personal electronic devices in an unsecure manor. All records or files containing personal information and/or student record information that are transmitted, including but not limited to, from one building to another building within the Cambridge Public Schools, must be transported in a sealed envelope/container or transported in any other reasonable and appropriate security procedures and practices necessary to protect personal information and/or student record information from unauthorized access, destruction, use, modification, disclosure or loss and all electronic records or files must be transported in an encrypted manner, and all records or files containing personal information and/or student record information that are transmitted from the Cambridge Public Schools to any third party must be accompanied by the requisite release, subpoena or court order, applicable contract provisions or applicable federal or state law and transported in a sealed envelope/container or transported in any other reasonable and appropriate security procedures and practices necessary to protect personal information and/or student record information from unauthorized access, destruction, use, modification, disclosure or loss and all electronic records or files must be transported in an encrypted manner.

o. All mobile electronic devices, including without limitation, laptops, will have in place a service that will allow them to wipe

the hard drive on any stolen laptop or mobile electronic device remotely and have purchased locks for all laptops and mobile electronic devices and have a protocol in place to ensure use by employees.

VII. External Risks

The following measures are mandatory and effective immediately in order to combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information and/or student record information, and evaluating and improving the effectiveness of the current safeguards.

a. There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of all personal information and/or student record information.

b. There must be reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information and/or student record information.

c. To the extent technologically feasible, all personal information and/or student record information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly to the extent technically feasible. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulations by the Office of Consumer Affairs and Business Regulation.

d. All computer systems must be monitored for unauthorized use of or access to personal information and/or student record information.

e. There must be secure user authentication protocols in place, including: (1) protocols for control of user ID's and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect, (4) restriction of access to active users and active user

accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts to gain access.

f. The secure access control measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to personal information and/or student record information.

g. All contracts or service agreements with third parties, including without limitation, all contracts and service agreements with third parties to perform institutional functions and services for CPS and all approved research projects and studies with third parties who will access to or will use, disseminate, store, transmit or retain or destroy files or records containing personal information and/or student record information will certify that they are in compliance with the provisions of M.G.L.c. 93H and the regulations promulgated thereunder as well as any other federal or state laws governing the protection of personal information and/or student record information and will certify that they have reviewed and complied with all information security programs, plans, guidelines, standards and policies that apply to the work they will be performing, that they will communicate these provisions to and enforce them against their subcontractors and will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information and/or student record information from unauthorized access, destruction, use, modification, disclosure or loss. At a minimum, third parties will represent that if personal information and/or student record information is to be stored on a laptop or other mobile electronic device, that such electronic devices are encrypted and that all such devices will be scanned at the completion of any contract or service agreement and/or research study or project to ensure that no personal information and/or student record information is stored on such electronic devices. Additionally, all third parties will sign a certification representing and warranting that they have in place a service that will allow them to wipe the hard drive on any stolen laptop or mobile electronic device remotely and have purchased locks for all laptops and mobile electronic devices and have a protocol in place to ensure use by employees. Preparation and execution of the necessary agreements to ensure confidentiality of data will be coordinated in conjunction with the Chief Information Officer, Deputy Superintendent for Teaching & Learning, and Legal Counsel.

Last date updated: May 15, 2018