Cambridge Public Schools
Administrative Guidelines and Procedures

TECHNOLOGY USE

The following guidelines and procedures address the acquisition, use, installation and update, and support of technology within the Cambridge Public Schools ("CPS").

Technology-related purchases

All technology related purchases, whether hardware, software, peripherals, on-line applications, services, and/or subscriptions must first be approved by Information, Communication and Technology Services ("ICTS"). In order to submit a request for approval, a purchase request form must be completed and submitted to purchasing. These forms can be found online under staff resources/on line forms.

Installation and Updating of Software and Hardware

All software installation and updates on Cambridge Public Schools technological resources must be performed by ICTS staff. Software and hardware will not be installed and/or updated if it was not previously approved by ICTS. Additionally, consistent with the CPS' Software Code of Ethics and Intellectual Property/Copyright policies, software and hardware will not be installed and/or updated if a proper license for the installation and/or update of the software is not on file with ICTS.

Users may not connect or install any computer peripherals or software which is their own personal property to or on the Cambridge Public Schools' technological resources without the prior approval of ICTS and the individual's immediate supervisor. Users may not download any material or software from the Internet for which a fee or license agreement is required without the approval of ICTS and appropriate building or district level administrators. Failure to comply with these requirements may result in a staff person being subjected to discipline, up to and including termination.

Email

All use of email must be in accordance with the CPS' Acceptable Use Policy. Staff should use the email account provided to them by the CPS for all school-related business.

Web 2.0 Approval Procedures

All use of Web 2.0 technology must first be approved by ICTS before it can be used within CPS. In order to submit a request for approval, users should initially review the Approved Web 2.0 Approved Web Applications to ensure their application is not an already approved resource. If it is not listed then, users should visit the school district web site to fill out the Web 2.0 Application Request Form. The submitted information will then be sent to ICTS for approval.

Donations of Technology to Schools

In accordance with the requirements of the CPS' Public Gifts to Schools policy, only the Superintendent of Schools may accept a gift or donation to a school and any such gift or donation only will be accepted if the gift or donation has an educational value. Information relating to any proposed gift

or donation of technology should be directed to ICTS for initial review. In connection with this submission, the manufacturer and specifications should be provided to ICTS.

After review, ICTS will forward the information to the Superintendent of Schools with a recommendation as to whether the gift or donation should be accepted. The Superintendent of Schools will then make a final determination as to whether to accept the proposed donation or gift.

In general, gifts or donations of hardware will not be accepted by the CPS unless the hardware aligns with current standards and is in good working order.

Disposal or Donation of CPS Technology

CPS technology must be returned to ICTS in order to be properly recycled, disposed of, and/or donated in accordance with the applicable federal, state, and local legal requirements. Individual staff and/or schools may not recycle, dispose of, and/or donate CPS technology. Failure to comply with this requirement may result in a staff person being subjected to discipline, up to and including termination.

Use of Personal Electronic Devices within CPS

The use of personal electronic devices for the recording, filming, photographing, audiotaping or videotaping of students by CPS is not permitted. All recording, filming, photographing, audiotaping or videotaping of students by CPS staff must be done on CPS-owned equipment. Additionally, only students who have a current signed media release on file may be recorded, filmed, photographed, audiotaped or videotaped.

Staff who use personal electronic devices within CPS are responsible for the safety and security of those devices. The City of Cambridge, CPS, and Cambridge School Committee and their respective officers, members, agents, representatives, and employees will not be responsible for any personal devices that are lost, stolen, or damaged in any manner. Responsibility for the maintenance and repair of personal devices rests solely with the owner. CPS will not provide technical support for any personal devices that are used within CPS. Any personal device that can connect in any way to the Cambridge Public Schools' network is considered a computing device subject to the Cambridge Public Schools Acceptable Use Policy and these Technology Use Administrative Procedures and Guidelines, and any other applicable policies and procedures and Cambridge Public Schools retains the right to determine when and where such computing devices may be connected to the network.

Technical Support

ICTS only provides technical support for CPS technological resources; technical support will not be provided for any personal devices that are used within CPS.

Protection of CPS Data

Access to records containing personal information (whether personal information of students or employees) 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 Cambridge Public Schools to comply with federal and state law and regulations. All data containing personal 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. 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. 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.

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 applicable state or federal record retention and destruction requirements. Before disposing of any such records, ICTS, the Office of the Chief Operating Officer, and the Office of Legal Counsel should be consulted to ensure that it is permissible for the records to be disposed of and to ensure appropriate disposal methods are adhered to.

Employees are encouraged to report any suspicious or unauthorized use of personal information to their immediate supervisor and to the Office of the Deputy Superintendent of Teaching & Learning if the use involves student record information and to the Executive Director of Human Resources if the use involves employee record information.

Whenever there is a security breach the Chief Operating 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, and 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 for which the office is responsible.

Access to electronically stored personal information (whether student record information or employee 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. Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks. At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with these Technology Use Administrative Procedures and Guidelines and Student Record Administrative Guidelines for protecting the security of personal information.

Terminated or temporary employees must return all records containing personal 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.) at the expiration of their employment with Cambridge Public Schools. A terminated or temporary employee's physical and electronic access to personal information must be immediately blocked. At the time of departure from employment in the Cambridge Public Schools, individuals shall be required to surrender all keys, CPS-owned equipment and electronic devices, and access codes that permit access to the office or information, and the individual's remote electronic access to personal information must be disabled, including without limitation, invalidating their voicemail access, Internet access, email access, and passwords.

Passwords to networks and programs are to be used exclusively by the authorized user of the password. Passwords should never be shared with others and should be changed at least every six (6) months. Passwords must be at least eight characters in length and include both alpha and numeric

characters. An authorized user should never allow anyone to access the network under their own password. Authorized users of a password are responsible for actions taken using that password, including transmission and receipt of information. Users who are provided with access to restricted information and files are expected to maintain the confidentiality of such information and exercise care to prevent unauthorized persons from gaining access to such information and files. Additionally, authorized users shall not modify files, other data, or passwords belonging to other users, or misrepresent other users on the network. Authorized users are expected to inform ICTS and their immediate supervisor of any unauthorized use of their password, any unauthorized installation of software or hardware or other technological devices, the receipt of inappropriate electronic transmissions, copyright violations, and any other inappropriate issues involving the use of CPS technological resources.

Employees are prohibited from transmitting or downloading records containing personal information onto their own home or personal electronic devices. All records or files containing personal information that are transmitted from one building to another building within CPS must be transported in a sealed envelope/container or transported using any other reasonable and appropriate security procedures and practices necessary to protect personal information from unauthorized access, destruction, use, modification, disclosure, or loss. All electronic records or files must be transported in an encrypted manner on CPS-issued devices. CPS provides multiple approved data transport methods, such as CPS email, collaborative sharing sites, and network shares, all of which are considered encrypted and approved methods of sharing within CPS. All records or files containing personal information that are transmitted from CPS 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 using any other reasonable and appropriate security procedures and practices necessary to protect personal information from unauthorized access, destruction, use, modification, disclosure, or loss and all electronic records or files must be transported in an encrypted manner.

Disciplinary Action

If it is determined that there has been a violation of the provisions of these technology use administrative procedures and guidelines by a CPS employee or student, CPS will take action that is appropriate under the circumstances. Action may range from discipline, up to and including termination or expulsion.

Date issued: May 15, 2018