NEW GUIDELINE - TECHNOLOGY UPDATE

INFORMATION SECURITY RESPONSIBILITIES

The District collects and maintains large amounts of data/information that must be protected and preserved.

To strengthen security of District Technology Resources (see definition Bylaw 0100) and Information Resources (see definition Bylaw 0100), the District has developed a series of information security policies available through the District's website. For the full text of these policies, please see _____ **[link]**.

For user convenience, a brief summary of the key requirements of these policies follows. Please address any questions to the District's Information Technology Office at _____ **[specify e-mail address]** or call _____ **[specify phone number]**.

All computer users are required to certify annually that (1) they have read the information security policies identified in this document, and (2) they understand and agree to abide by the information security policies applicable to them. Appropriate training will be provided to all users. **( )** In addition, all users with access to the District's protected health information or personally-identifiable information (e.g., social security numbers, credit/debit card information, etc.) are required to affirm that they will not store this information on mobile/portable storage devices without (1) obtaining prior authorization from the Superintendent, and (2) encrypting the data.

Expectations for All Technology Users

This document summarizes the Board of Education's information security policies. Users of the District Technology Resources must read these summaries, and both understand and fulfill their responsibilities under the applicable policies.

A. In many cases, operating system and application updates, along with malware protection, are all that stand between a computer and a system compromise or infection. The District Technology Resources are regularly updated and provided malware protection.

[ ] Users are responsible for verifying their computers are configured to receive automated patches, and ensuring the automated updates run so that security vulnerabilities are patched in a timely manner.

[ ] Users must also verify their malware protection is properly installed, updated, and is running the latest virus definitions.

[ ] Users' school or department IT support staff is available to assist with these responsibilities.

[NOTE: END OF OPTION LANGUAGE; THE THIRD OPTION SHOULD BE SELECTED IF THE FIRST AND/OR SECOND OPTIONS ARE SELECTED.]

If District users access District Technology Resources using personal communication devices, they must verify proper security measures are active on their devices.

B. No software is 100% effective in preventing compromises or infections, and not all websites are safe. Users must be alert when using the Internet, especially on systems storing or processing protected and confidential data/information. One way to reduce the risk of compromise is to limit the user's non-work related Internet activity.

C. **[DRAFTING NOTE: SELECTION OPTION #1 OR OPTION #2]**

[ ] [OPTION #1]

Unless authorized and using a device that is capable of encrypting the data/information, users are prohibited from storing District Confidential Data/Information on the user's computing devices.

[END OF OPTION #1]

[ ] [OPTION #2]

Because confidential data/information exists in many forms (e.g., written, spoken, electronically recorded, printed, etc.) users are responsible for properly securing this data/information at all times. This may take the form of physical security (e.g., locked cabinets, locked doors, locked building) or through digital security (e.g., passwords, biometric authentication, encryption). All users with access to the District's Confidential Data/Information are:

( ) prohibited from storing this data/information on any mobile computing device (e.g., laptop, tablet) or portable storage device (e.g., flash drive) that is not encrypted;

( ) required to activate their devices' available security feature(s) that prevent direct access to the data/information on the device without first verifying the identity of the user via a secure method (e.g., passcodes, biometrics, user id/password). This applies to both personal and District-provided devices when District Confidential Data/Information may be stored on that device (e.g., e-mail, student records, etc.). Users are prohibited from storing District Confidential Data/Information on any device that does not meet this basic level of security;

( ) prohibited from storing Confidential Data/Information on any mobile /portable storage device (e.g., USB flash cards, CD-ROMs, etc.)

( ) prohibited from storing Confidential Data/Information on any mobile /portable storage device (e.g., USB flash cards, CD-ROMs, etc.) that is not encrypted;

( ) prohibited from storing Confidential Data/Information on any mobile /portable storage device (e.g., USB flash cards, CD-ROMs, etc.) that is not encrypted or password protected;

( ) allowed to store Confidential Data/Information on the District provided cloud storage (e.g., Microsoft OneDrive). Use of other public cloud storage options for Confidential Data/Information is prohibited.

[END OF OPTION #2]

D. District Confidential Data/Information includes many different types of data/information, such as social security numbers, personal health information, student records, and bank and credit card information, or other personally-identifiable information.

E. District Confidential Data/Information must never be shared through instant messaging or peer-to-peer (P2P) file-sharing software or devices. P2P software must never be installed on machines or devices that store, process, or access confidential data/information. District users are required to obey copyright laws and to adhere to the acceptable use policy (Policy 7540.03 and Policy 7540.04).

F. District Confidential Data/Information must be accessed only through one (1) of the following methods: (1) user authentication with the correct password; (2) multi-factor authentication, such as a smart card in combination with a password; or (3) biometric identification approved by the District's Information Technology Office. **[OPTIONS] ( )** Some networked storage options supplied by the District are not suitable for the storage of District Confidential Data/Information because they do not conform to these access requirements. **( )** Likewise, third party consumer cloud computing or software-as-a-service offerings such as Dropbox, Google Docs, iCloud, and other similar offerings are not acceptable for the storage of District Confidential Data/Information unless the District has a current contract with these providers that includes data/information security. **[END OF OPTIONS]** If a user is not sure if a storage location is secure, the user should contact the District's Technology Office.

G. Machines and devices that store District Confidential Data/Information, or that are used to access mission critical systems (e.g., SIS, ERP, Payroll), must be used only in areas with restricted or controlled access and must be locked whenever they are left unattended. Machines and devices containing District Confidential Data/Information or used to access mission critical systems and resources must be set to require re-authentication after not more than _____ (_____) minutes of inactivity. **( )** It is recognized that requiring re-authentication for teachers every _____ minutes may be disruptive to teaching. Therefore, it is the teacher's responsibility to appropriately protect Confidential Data/Information in the classroom by ensuring students, parents, volunteers, visitors, or others without authorization to view/access the data/information do not view/access it when the Confidential Data/Information is in use.

H. District Confidential Data/Information maintained on computers or other electronic devices should be destroyed or disposed of only in accordance with Board policy and State law. Any school or department intending to surplus computing devices and or printer/copy machines or any other device that stores information must first destroy the electronic information by wiping the data from the hard drive(s), flash storage, or having this done by authorized District personnel and keeping the devices physically secure until transfer to District Surplus.

I. Users must maintain strong passwords for every District system and application they access that stores/processes District data/information. Users must change all passwords used for District systems in accordance with the District's password requirements.

J. Per the Board's e-mail policy, users must always use their official District-supplied e-mail address for official business. Auto-forwarding of District e-mail accounts is prohibited **( )**, unless approved by the Superintendent. Manual forwarding of individual e-mail messages is permitted.

K. Users must immediately report lost or stolen mobile/portable devices (e.g., laptops, smartphones) or security breaches (e.g., computer viruses, hacking attempts) to the District's Information Technology Office and/or the District Security Office. If a user suspects District Confidential Data/Information or mission critical systems and resources are at risk, the user must make this point clear when submitting a report. Also, if a user suspects District Confidential Data/Information is at risk, the user should avoid taking any actions such as manually scanning the computer with antivirus software. Information Technology and/or Security employees will assess what needs to be done.

L. Users must be mindful of the risks associated with District Confidential Data/Information when storing, processing, or accessing data/information. If a user is not sure how to comply fully with Board policies or procedures or if the user is not sure how to conduct a process securely, the user should ask for assistance from the site or department IT support contact or the District's Information Technology Office. Users are expected to know their sites' information technology contact so that they can contact him/her when there is a need.

Expectations for Administrative Personnel

In addition to the preceding, administrative personnel must also understand and fulfill the following responsibilities. Appropriate training will be provided.

A. Each District site or department that is responsible for maintaining its Technology Resources and Information Resources must have a designated information technology contact, plus a designated backup information technology contact. The District's Information Technology Office monitors the duties, responsibilities, and training of information technology contacts. Each site or department administrator that maintains its own information technology must verify that its IT support personnel have been trained to maintain the unit's IT resources in compliance with all of the District's information security policies and procedures.

B. Each District site that stores District Confidential Data/Information or that operates mission critical systems must work with the District's Information Technology Office to perform regular vulnerability scans.

C. Each District site or department administrator that maintains its own information technology is responsible for reporting immediately to the District's Information Technology Office or Security Office any time there is reason to suspect that the security of District Confidential Data/Information or of a mission critical system (e.g., Human Resources, Finance, Student Information Services, Payroll, e-mail, etc.) has been compromised or is at risk.

Expectations for Technology Support Personnel

In addition to all of the above, technology personnel, regardless of the site to which they are assigned, must also understand and fulfill the following responsibilities. Appropriate training will be provided.

A. IT personnel must read, understand and comply with the Board's policies and procedures that govern the use, operation and protection of IT systems and resources. The information technology security standards described in the information security policy are minimum standards required for the protection of District systems, including those that store/process District Confidential Data/Information or that are considered mission critical. Site and department IT resources for which an IT support employee is responsible must be managed in compliance with these policies and procedures. If technology personnel have questions or need assistance, it is the employee's responsibility to contact his/her Principal and/or the District's Information Technology Office.

( ) Technology personnel managing mission critical systems and District Technology Resources (e.g., Human Resources, Finance, Student Information Services, Payroll, e-mail, etc.) or systems that store/process District Confidential Data/Information must have formal information security training. Information security training is available from the District's Information Technology Office.

B. IT personnel are responsible for enforcing District password requirements for the systems and applications the IT personnel manage. System and application administrators must configure all District-owned and managed IT devices/systems to implement the password requirements to the degree technically feasible, in compliance with the District's password standards.

C. If a user is unsure how to transfer District Confidential Data/Information, the user should contact the site/department technology contact for assistance. If the site/department technology contact is unsure of the proper method to transfer the Confidential Data/Information, the request should be referred to the District's Information Technology Office.

D. IT personnel must report system and application vulnerabilities to the Principal and/or the District's Information Technology Office.

E. The District Information Technology Office will perform regular vulnerability scans of District Technology Resources.

F. If technology personnel suspect that the security of any data/information or of a mission critical system (e.g., Human Resources, Finance, Student Information Services, Payroll, e-mail, etc.) has been compromised or is at risk, it is their responsibility to report that immediately to the District's Information Technology Office and/or Security Office. No action should be taken that might inhibit investigation of an incident or make unavailable information that might assist the investigation.

G. Technology personnel are required to follow incident handling instructions as specified in the incident management policy and/or as directed by the District's Information Technology Office or Security Office in response to potentially unauthorized access of protected information.

Key Information Security Policies and Administrative Procedures

Below are brief descriptions of the District's policies and procedures related to information security. The full text of each policy or procedure can be found on the District's website or by clicking the highlighted link.

Policies

A. Policy 7540 – Technology – Authorizes the development of a District Technology Plan to facilitate effective use of District Technology Resources that support student learning and/or District business operations.

B. Policy 7540.02 – Web Content, Services and Apps – Addresses the requirements for creation of District-authorized websites, services and apps by employees and students.

C. Policy 7540.03 – Student Technology Acceptable Use and Safety - Describes student use of District Technology Resources, expectations of privacy, District technology protection measures, areas for student training, and assigned school e-mail accounts.

D. Policy 7540.04 – Staff Technology Acceptable Use and Safety - Describes staff use of District Technology Resources.

E. Policy 7540.05 – District-Issued Staff E-mail Account and Policy 7540.06 – District-Issued Student E-mail Account - Establishes a framework for proper use of District issued e-mail accounts as an official business or educational tool for staff and students.

F. Policy 8305 – Information Security – The Board authorizes the Superintendent to develop internal controls necessary to provide for the proper collection, classification, retention, access, and security of data/information to include procedures in the event of an unauthorized release of information and training for staff.

Administrative Guidelines

A. AG 8305A – Information Security Responsibilities and Policy 8305 - Information Security - Review of what every computer user, administrator, and technology support employee should know in order to ensure the security of District information.

B. AG 7540B– Technology Director – and Policy 7540 – Technology - Describes the responsibilities for the position of Technology Director.

C. AG 7540C – Technology Governance Committee – Presents the requirements for establishing a District Technology Governance Committee that will create standards and procedures for proper management and protection of District technology resources.

D. AG 7540A – Staff and Student Training Regarding the Internet - Describes areas to be included in training of staff and student in proper use of the Internet.

E. AG 8305 – Collection, Classification, Retention, Access and Security of District Data/Information – Provides a framework that District employees can use to classify data/information for the purpose of determining the data/information's need for protection.

F. AG 8305B - Information Security Incident Management – Presents requirements for managing and reporting information security incidents.