SUPPORT OPERATIONS 5301

PURPOSE, USE AND ADMINISTRATION OF DISTRICT DIGITAL INFORMATION SYSTEMS

I. Scope of Policy

A. Digital information systems are important to achieving the District's educational goals and conducting business operations in an efficient manner. The Board's goal is to provide students and staff with digital technology tools that are appropriate to support the District's instructional goals and operational needs, consistent with a wise use of the District's financial resources.

B. When used in this Policy, the term "digital information systems" includes computers of any size and form factor (including smartphones and tablets), network servers, routers, cables, interactive white boards, video conferencing equipment, switches, and software that is owned, leased, or licensed by the District, or that the District has the use of through a cooperative educational services agreement (CoSer), and that is used to create, modify, store, or transmit information in a digitized form.

C. This Policy applies to the use of all District-managed devices, including mobile devices such as laptop computers and digital tablets, whether the equipment is used by staff, students, or members of the public. References to District-managed devices shall include devices owned by the District and devices that may continue to be owned by the BOCES but are assigned to the District for use within the District under District supervision.

D. This Policy also applies to the use of digital devices that are not District-managed devices but are used to access and connect to the District's network, whether the device is owned or used by a staff member, student, or member of the public.

E. Anyone who uses any part of the District's digital information systems is expected to comply with the standards of use set forth in this Policy, whether that person is a staff member (employees and volunteers), student, contractor, or member of the public (including parents and community members).

F. In addition to the standards set forth in this Policy for use of the District's digital information systems, users of those systems must comply with all other board-adopted policies and related regulations, including but not limited to, the Code of Conduct, the Internet Safety Policy, and the Equal Opportunity and No Workplace Harassment Policy.

II. District Accountability for Use of Digital Information Systems

A. The Board recognizes the District's responsibility to monitor the use of its digital information assets to insure that those assets are used for their intended purposes, and

that the use of those assets does not expose the District to unnecessary risk. The Superintendent shall develop procedures and operating protocols that provide for the periodic review of access logs and filtering logs for the purpose of identifying possible misuse of the District's assets.

B. The District reserves the right to inspect the contents of any digital files, folders, images, or other digital information created, modified, stored, or transmitted using the District's digital information assets.

1. The only information that should be created, modified, stored, or transmitted using the District's digital information systems is information that is necessary to or supportive of the District's education program or business operations. Individuals do not have an expectation of personal privacy in any information created, stored, or transmitted by the individual using the District's digital information systems. This includes any passwords to an individual's personal internet accounts that the individual chooses to store on the District's digital information systems.

2. The Superintendent shall insure that staff, students, and the public are periodically advised that any information created, modified, stored, or transmitted using the District's digital information systems may be examined by the District for such reasons as to insure that the systems are being properly used, or to comply with obligations under laws such as the Freedom of Information Law (FOIL), the Family Educational Rights and Privacy Act (FERPA), and litigation discovery procedures.

C. The District is not responsible for the quality, availability, accuracy, nature, or reliability of Internet service beyond the point at which the District's digital information systems connect to the Internet. Not all information found on the Internet is accurate or reliable, and each user is responsible for verifying the integrity and authenticity of information that the user finds on the Internet.

D. The District maintains its digital information systems for the sole purpose of delivering its educational program and conducting its business operations, and the digital information system shall not be deemed to be a public forum or limited public forum.

III. Responsible Use of Digital Information Systems

A. Instructional and non-instructional staff are provided with access to the District's digital information systems for the purpose of performing their work duties. Use of the systems for any other purpose may be classified as unacceptable work performance, and may be subject to counseling or discipline consistent with

applicable laws and collective bargaining agreements. Limited personal use for such purposes as brief communication with family members may be acceptable, but staff members should keep in mind that any data created by personal use remains subject to review by the District.

B. Students are provided with access to the District's digital information systems for the purpose of completing instructional assignments under the guidance of a teacher. Use of the systems in a manner that does not comply with the standards in this Policy or another Policy, or guidance issued by the Superintendent or other administrator or teacher, may result in disciplinary action consistent with the District's Code of Conduct.

C. Members of the public may access the District's digital information systems to support a child's education (e.g., Parent Portal to access grades), to communicate with staff, or for personal reasons (e.g., WiFi access while in the school building). The Superintendent, in consultation with the Director of Instructional Technology, shall develop and implement procedures and protocols so that members of the public are reasonably advised of their responsibility to adhere to the standards set forth in this and other Board Policies, and are reasonably advised that information created, modified, stored, or transmitted through the District's digital information systems is not considered private, except to the extent explicitly provided by law.

D. Users must not engage in conduct that may compromise the security of the District's digital information systems.

1. A user may not access the systems with any password other than the password given to the user by the authorized District staff member.

2. A user may not disclose the user's assigned password to anyone except a District staff member authorized to have access to that user's password.

3. A user may not download or install any program, app, content, or other software that has not been approved for installation by the District.

4. A user may not circumvent, or attempt to circumvent, any computer security measure implemented by the District or required by any service provider or program as a condition for using a service or program.

5. A user may not download, create, or distribute a virus, Trojan horse, adware, or other malware, or add files to or delete files that change the function or operation of the digital information systems.

E. Users must understand and respect the capacity of the digital information systems and the need to accommodate other users. Therefore, users shall not engage in activities that use a disproportionate share of the system's assets, such as creating or disseminating commercial advertising, political fundraising, mass mailings (unless pre-approved school-related purposes), or playing online games that have not been incorporated into course material.

F. Users must respect the rights of other individuals regarding content those individuals have created. A user cannot download or use content in violation of copyright laws, including music, movies, artwork, photographs, and programs.

G. Users may not access, upload, download, or distribute pornographic material, obscene material, or sexually explicit material.

H. Users may not create or distribute information that is disrespectful of other persons or groups, or that is illegal, defamatory, abusive, intimidating, harassing, or bullying, or the creation or distribution of which is illegal.

I. Users may not participate in chat rooms, instant messaging, or e-mail that is not specifically permitted by a staff member as a legitimate school-related purpose.

J. Users may not send or display unsolicited non-educational related messages or pictures.

K. Users may not access the internal components of a computer or other device, except as instructed by an authorized member of the District's instructional technology staff or other technical consultants.

L. Users may not access, or "hack into," other user accounts or files or directories that the user is not authorized to access.

M. Users may not use the District's digital information systems to conduct business transactions not related to their school responsibilities, or to perform work on behalf of any non-school organization.

N. Users may not engage in any activity using the District's digital information systems that violates any local, State, or federal law.

O. Users who engage in inappropriate use of the digital information systems may have their access rights modified or revoked, or be subject to discipline consistent with the District's Code of Conduct and applicable laws and collective bargaining agreements.

IV. Physical Environment and Security

PURPOSE, USE AND ADMINISTRATION OF DISTRICT DIGITAL INFORMATION SYSTEMS

A. The physical assets that are incorporated into the District's digital information systems (hardware) are both valuable and vulnerable. To the extent feasible in existing facilities, network servers and other critical infrastructure shall be installed in physical locations that provide appropriate ventilation, electrical supply, and an absence of potential risks (e.g., water leaks). Future facility plans shall include consideration of proper physical spaces to house digital network infrastructure.

B. The Superintendent, in consultation with the Director of Instructional Technology, shall adopt a protocol for limiting access to spaces housing network servers and other critical infrastructure, and for logging the identity of those accessing those spaces and the dates of access.

C. If a District-managed mobile device is assigned to a student or staff member for their dedicated use, a record shall be made identifying the device, the person to whom it is assigned, the date of the assignment, and the date of the expected return of the device. All devices shall be returned to the Instructional Technology Department no later than June 30 of each school year, unless prior arrangements have been made with the IT Department.

D. A staff member or student may take possession of an assigned device only after providing the Instructional Technology Department with a written agreement acknowledging the following conditions with respect to the device and any related equipment provided with the device:

1. Use of the device must conform to the standards of responsible use set forth in this Policy, and all other applicable District policies and rules, whether the device is connected to the District's digital information systems or not;

2. The device remains the property of the District, and must be returned to the District at the designated time or when the user ceases to be affiliated with the District, if earlier;

3. The user will take reasonable care to protect the device from damage due to dropping or other physical shock, inclement weather, spillage of food or other substances, and other physical dangers;

4. The user will lock the device using the assigned password, will not share that password with anyone other than an authorized District employee or designee, and will not allow any other person to use the device;

5. The software installed on the device is owned by or licensed to the District, and the user may not copy or alter the installed software; the user will not

install or download any software, program, application, or executable code onto the device that is not approved by an authorized District employee or designee;

6. The user acknowledges that the device may be equipped with software installed by the District to protect the device from damage from viruses or other malware, which may prevent the user from installing software or making other changes to the device, and the user agrees not to attempt to remove, neutralize, or circumvent this security measure;

7. The District retains the right to examine the device and its contents, and may do so remotely, and the user has no expectation of privacy in any information created, modified, stored, or transmitted with the device; and

8. If the device is damaged through the gross negligence of the user, the user will be responsible for compensating the District for the damage.

Where the user is a student, the acknowledgement shall be signed by both the student and a parent or person in parental relation.

V. User Access Rights

A. The District shall assign each user rights to access only those assets of the digital information systems, and only those data fields, files, or elements that are appropriate to the user's status and, where applicable, job responsibilities.

B. The District shall periodically review the roster of users and their assigned access rights, and make adjustments to reflect any changes in circumstances.

C. Users shall be required to use passwords that meet standards established by the Superintendent, in consultation with the Director of Instructional Technology, and to change passwords periodically.

D. The Superintendent, in consultation with the Director of Instructional Technology, is authorized to develop and adopt procedures and protocols for assigning, reviewing, and removing user access rights, including the use of passwords. These procedures and protocols shall include procedures for removing users from the roster when an individual is no longer affiliated with the District.

VI. Mitigation of Business Interruption Risk

A. The District shall create, periodically review, and update as necessary, a disaster recovery plan that provides a reasonably specific roadmap to responsible District

personnel of the steps to follow in responding to, and recovering from, a disaster-related interruption of the operation of the District's digital information systems. The plan shall be responsive to such extraordinary events as flood, storm, electrical grid failure, system component failure, and cyber intrusion.

B. As part of the disaster recovery plan, the District shall create, periodically review, and update as necessary, a plan for routine backup of the information stored in the District's digital information systems. The backup plan shall balance cost and administrative effort with the potential consequences of losing particular data elements. The importance of individual data elements or databases to the continued operation of the District shall be prioritized and backup schedules set accordingly.

C. The Superintendent, in consultation with the Director of Instructional Technology, is authorized to develop and implement the procedures and protocols for disaster recovery and information backups. The Board shall be briefed on the status of these plans at least annually.

VII. Email Component of Digital Information Systems

A. All references in this Policy to the use of District digital information systems include the use of those systems for the composing, sending, receipt, and storage of email. The District's reserved right to access and inspect information stored on or passing through its systems applies to email messages and related metadata. The standards of responsible use set forth above apply to email.

B. Use of Email By Staff Members

1. Staff members are provided with credentials to access and use the District's email domain (@District/BOCEScsd.org) to send and receive work-related emails. As noted above, those emails are not confidential or private. The District may review those emails for any reasonable business purpose, including to insure compliance with this and other Policies, and with other applicable laws and regulations. The District may be required to disclose emails to third parties pursuant to FOIL, FERPA, or other legal requirements. Employees shall not conduct personal business using the District's email address.

2. Staff members must use the District's email domain to send and receive all work-related messages. If a staff member uses a personal email account to send or receive a work-related message, the staff member may be required to provide access to the personal email account in order to comply with FOIL, FERPA, or another legal requirement.

3. If a staff member stores personal email, or passwords to personal email accounts, on the District's digital information systems, that information will be available to the District.

4. Each email is a business document. Consistent with the standards for responsible use set forth above, all email should be businesslike, appropriate to the business purpose, and respectful of the recipients. Staff members must keep in mind that every email is subject to public disclosure under FOIL.

5. Emails that contain personally identifiable student information may be classified as education records under FERPA. Staff members should use discretion when communicating personally identifiable student information to anyone through email. Disclosure of personally identifiable student information to other staff members should be limited to those staff members who work with the student.

C. Use of Email by Students

1. Use of the District's email domain by students is permitted when assigned by a teacher as part of a class requirement, project, or unit.

2. Students may not access their personal email accounts (such as Yahoo!, MSN, personal Gmail, etc.) through a District-owned machine.

3. The District's email domain is filtered and can be monitored by school staff. Students do not have an expectation of privacy when using the District's email domain.

VIII. Personally-Owned Devices Connected to the District's Digital Information Systems

A. When devices not owned or managed by the District access the District's digital information systems, the District is exposed to several additional risks, such as the risk that malware will infiltrate the District's system from a non-secure device; the risk that confidential student information will migrate to the device, which might then be lost or stolen; and the risk that records relating to District business will be stored on the device, and the District will be legally obligated to produce those records in response to a FOIL request or litigation. To mitigate these risks, employees connecting non-District managed devices to the District's digital information systems shall be required to accept certain requirements.

B. The Superintendent, in consultation with the Director of Instructional Technology, shall develop and implement procedures and protocols for authorizing devices not managed by the District to be connected to the District's digital information systems.

PURPOSE, USE AND ADMINISTRATION OF DISTRICT DIGITAL INFORMATION SYSTEMS

Devices shall not be connected to the District's systems unless the user of the device agrees to the terms determined by the Superintendent to be appropriate and necessary to mitigate the foreseeable risks. Those terms shall include, but not be limited to:

1. The user acknowledges familiarity with this Policy and other relevant Policies, and agrees that the use of the District's digital information systems through the device will comply with the standards of responsible use and other requirements in the Policies;

2. The user agrees to give the District access to the memory of the device when the District has a business reason to retrieve data or documents, including the need to respond to a FOIL request, a request for education records under FERPA, or a litigation disclosure requirement, or a review to confirm compliance with the standards of responsible use;

3. The user agrees that no District-related data or documents will be copied or otherwise stored in personal "cloud" accounts such as Dropbox, Box, OneDrive, etc.;

4. The user agrees that District-related communications will be sent and received as email when practicable, and that text messaging will only be used to relay non-essential information;

5. In the event that the device is lost, stolen, or missing for more than 48 hours, the user will immediately notify the Director of Instructional Technology, and will cooperate with all District efforts to recover or reconstruct District-related information that was stored on the device;

6. The user acknowledges that if the device is used to access the internet through the District's digital information systems then that access will be filtered in accordance with the District's Internet Safety Policy;

7. The user agrees that all system updates and all application updates will be installed within a reasonable time of being available, and agrees that anti-virus software will be installed on the device, activated, and updated where applicable;

8. The user agrees that, if the device has the capability to connect to the internet using cell phone (3G/4G) connections, the user will not connect the device to the internet using that capability while on school premises. Instead, the user will always connect to the District network in order to connect to the Internet;

9. The user agrees that the District will not be responsible for any damage that occurs to any component of the device, including processors, memory, video displays, WiFi or Bluetooth circuitry, or programs as a result of being connected to and operating on the District's digital information systems; and

10. The user agrees that failure to abide by the terms of use will be sufficient reason for the District to block the device from further access to the District's digital information systems.

C. The use of non-District managed devices by students on school property shall be subject to rules and protocols approved by the Superintendent after consultation with building principals and teachers.

IX. Student Data Security and Parental Consent

A. The creation, modification, storage, and transmission of personally identifiable student information using the District's digital information systems must comply with the requirements of federal and State law.

1. Usernames and passwords assigned to or created for students will generally be considered personally identifiable student information.

2. Personally identifiable student information may not be provided to third party contractors (including online or "cloud" services) without determining that any online Terms of Service or other online agreement complies with federal and state laws. The Superintendent shall develop and implement a procedure for administrators, teachers, and other staff to seek evaluation of any online product or service that they wish to implement to support instruction or business operations.

B. The standard procedure in the District shall be to provide each student with access to the District's digital information systems unless student violates the District rules for the use of those systems or the District is notified in writing (including email) by a student's parent or person in parental relation that the student is not to be given access to those systems. At the time of enrollment and the beginning of each school year, a student's parent or person in parental relation shall be notified of this Policy, the importance of online access to contemporary education methods, and how to inform the District that their student is not to be given access to the District's digital information systems.

X. Data Security Awareness Training

PURPOSE, USE AND ADMINISTRATION OF DISTRICT DIGITAL INFORMATION SYSTEMS

District staff shall be provided with instruction concerning the requirements of applicable laws and this Policy, and the importance of following best practices to protect the security of information stored in the District's digital information systems.

Oriskany Central School District
Cross Ref: Equal Opportunity and Nondiscrimination
Code of Conduct
Internet Safety
Adopted 03/13/17