SOUTH COLONIE **4526.2**

TECHNOLOGY USE POLICY FOR STAFF MEMBERS

Implementation of the District's Technology Use Policy

It is important that all users have the opportunity to review, ask questions about and understand the Technology Use Policy. During each school year, the Technology Use Policy will be reviewed with all staff. Changes will be distributed as it is revised each year. New staff will have the opportunity to review this document and ask questions about its content during staff orientation.

Staff Use of District Computer Network System Resources

The Board of Education encourages staff to make use of the District's network to explore educational sites, conduct research, participate in professional development and contact others with similar educational interests.

The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent of Schools or his/her designee(s) to provide staff with training in the proper and effective use of the District's network systems technological tools that will increase student learning.

Generally, the same standards of acceptable staff conduct that apply to any aspect of job performance shall apply to use of the District's technological/network system. Employees are expected to communicate in a professional manner consistent with applicable District policies, procedures, and regulations governing the behavior of school staff. Care should be taken in the use of electronic mail and telecommunications facilities to insure that confidential information about students or other employees remains private.

District staff shall adhere to all the laws, policies and rules governing computers and electronic devices including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

Staff members who engage in unacceptable use may lose access to the District's network/ technological system and may be subject to further discipline under the Civil Service Law, Education Law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who damages or destroys the technology tools of the District.

Privacy Rights

Information and data stored on District computers, electronic devices or network systems is and shall remain District property and are subject to District control and inspection. Appropriate staff members of the Information Technology Department will have access to all computers, electronic devices and networks to insure that users are complying with the requirements of this policy. Staff members should not expect that information stored on the District's hardware or network systems will be private.

Access to the Internet

All District employees shall complete Employee Account Agreements as well as Network Access Agreements prior to gaining access to any District technology resources or networks, including intranet, internet and Wi-Fi access.

Remote Access

Any and all remote access accounts shall be reviewed by appropriate school administrators and, if appropriate, forwarded for implementation to the Information Technology Department. The District shall evaluate overall cost, utilization, and purpose.

Internet (including public Wi-Fi)

It shall be each individual user's personal responsibility to be aware of the potential for, and possible effects of, manipulating electronic information and to verify the integrity and authenticity of information that he or she compiles and utilizes from the Internet. The Information Technology Department retains the right to monitor internet use.

Each individual user is responsible:

- to recognize and respect the diversity of the population and the opinions of other Internet users;
- to behave ethically; and
- to comply with the legal restrictions regarding the use of the information resources.

Disseminating information that is illegal, defamatory, abusive, threatening, racially offensive and/or adult-oriented will be deemed a violation of this policy, as will accessing information that is adult-oriented or illegal, and such behavior will result in disciplinary action against the violator pursuant to the Civil Service Law, Education Law or in accordance with applicable collective bargaining agreements.

E-Mail

For appropriate staff members, the District will make e-mail accounts available. The use of these accounts will be strictly limited to communication in support of the instructional, non-instructional and administrative work of the District. Since all students do not have equal access to technology outside of school, the instructional application of e-mail will be supplemental to, and not in lieu of, other District-supplied instructional resources.

The following is a list of specific system-use requirements that apply to all users of system-wide networked resources regardless of building, platform, operating system, and application.

1. Only District Technology Staff is authorized to make hardware or software configuration changes to any networked or stand-alone resources. These changes include:

    - The installation or de-installation of software applications.
    - The installation or de-installation of workstation or network hardware.
    - The removal, relocation, addition or reconfiguration of any network element.

2. New software installations will not be made until the proposed software:

    - Has been recommended by content area experts.
    - Is approved by District Information Technology staff for network compatibility.
    - Is previewed by content area experts and district Information Technology staff.

3. Subject to the software review process, applications and other executable files may be installed on the server or workstation hard drive. Once installed, they will not be removed without additional software review.

4. The District Information Technology staff will identify network software, hardware, and other devices that will be supported district-wide.

5. Users will be assigned network home (H:) directories in which to store files created on the District system. This is the only location where users should store data that users expect to be backed up by District Information Technology staff. These directories will be limited in size subject to the nature of their use. This limit may be increased upon request, with supervisor approval.

6. The Information Technology staff is not responsible for data stored in locations other than the user's server-based home (H:) directory. This includes data stored on flash drives, hard drives (C: drive), writable CD, DVD and other storage or removable media.

7. Only the files stored on District servers may be backed up by District Information Technology staff. Since storage space is limited, users will be required to purge their files on a regular basis. With notice, District Information Technology staff may also remove files on a regular basis. District Information Technology staff will analyze and, if appropriate, provide assistance in backing up data files upon request.

8. Files created and stored on the District system are subject to review by authorized District staff. These documents may also be subject to access as a result of formal Freedom of Information Law (FOIL) requests and other legally enforceable access requests.

9. Unauthorized access to any part of the District network is strictly prohibited and may result in the loss of system privileges, district-imposed discipline, or legal action.

10. Since any removable media can be a ready source of viruses, the District may disable this access on a public access machines if it represents a virus threat.

11. Users will not access computer games from any source unless used as a part of an instructional program or activity authorized by the building principal.

12. Only screen savers included in the current workstation operating system can be installed on the desktop.

13. Staff access to the District network for any purpose will be password controlled.

14. No executable files in any form will be downloaded from the Internet or other outside sources or installed or stored on any District resources. This restriction includes on-line services or any other commercial, privately developed, locally developed, or experimental executable file, macro, or application.

15. All users of the District network are specifically prohibited from engaging in the following activities:

    - Sending or displaying offensive messages or pictures (i.e., pornography).
    - Using obscene language.
    - Harassing, insulting or threatening others.
    - Damaging computers, systems or networks.
    - Engaging in any acts of cyber-bullying
    - Violating copyright laws and the valid licensed rights of others.
    - Use of an account password by anyone other than the account holder.
    - Encrypting or password protecting material stored on the system.
    - Possessing programs used for hacking or stealing passwords.
    - Trespassing in another user's folders, work or files.
    - Not using resources in a thoughtful manner.
    - Employing the network for non-school related, commercial or other private purposes.

16. If it is necessary to download large files for appropriate academic reasons, staff should request permission through their Building Principal or his/her IT staff designee.

17. Upon termination of employment, the District Information Technology staff shall have the right to purge any and all associated accounts or data files of the former employee. Upon the anticipation of changes in staffing (e.g., retirement, change of position, termination, etc.), the District reserves the right to retain all data on any electronic equipment related to the position. Upon District review, if appropriate, the District will erase all non-essential (non-work related or non-position related) data within ninety (90) days of the former employee's date of departure from employment.

Cross-Reference: Cyber Bullying, Policy 4527
Code of Conduct, Policy 5300

Adopted: October 5, 2004

Revised: June 27, 2017; January 7, 2014

TECHNOLOGY USE FOR STAFF MEMBERS REGULATION

General Guidelines

Staff use of computers and electronic devices is for school-related business use only. Foreign or home software is permitted on hardware only with the express permission of the Information Technology Department. The District retains the right to review the contents of any data storage device and e-mail of any user. Network etiquette, consistent with the Code of Conduct, should be observed (e.g., no abusive language, inappropriate behavior, cyber bulling or illegal activities will be allowed).

Use of Electronic Research Activities

All materials over the Internet should be assumed to be copyrighted for citation purposes but the South Colonie School District has no responsibility for the accuracy or the quality of information obtained through Internet services. E-mail is not confidential and messages in question for legal reasons will be reported to the authorities. Use of another individual's account without permission from that individual is strictly prohibited. District owned account information is considered confidential.

Prohibited Activities

Staff members are not allowed to promote activities against District policies or local, state or federal laws. Prohibited use of the computers, electronic devices and computer services shall include, but not be limited to:

- subscriptions to "listservs" using school accounts without authorization
- hosting of "usenet" groups and "listservs" without authorization
- unauthorized copying of software
- lending or selling of software copies without express written permission from copyright holder with the exception of shareware or public domain software
- unauthorized downloading of information or applications onto District-owned hard drives or storage devices
- unauthorized attempts to access passwords of others
- unauthorized attempts to access or modify the system's programs
- any malicious attempt to destroy material of another user or the school district, including the uploading or creation of computer viruses and spyware
- harassment or cyber-bullying of others by e-mail or any other means of electronic communication
- loading of personal software by any means into the District's computers and/or network, without the knowledge or permission of the Teacher/Administrator or IT Department staff member
- sharing of passwords
- accessing secure data without authorization

Consequences of Inappropriate Use of District Hardware and/or Software

Failure to comply with any portion of these administrative regulations will result in disciplinary action including, but not limited to:

- school penalties, as appropriate
- where warranted, other civil or criminal proceedings

Notification of Changes in Technology Use Policy

The District's Technology Use Policy shall be made available on the District website and in the Main Office of all school buildings.

Staff will receive notification of changes to the Technology Use Policy electronically via e-mail. Any revisions will also be posted on the District website.

Cross-Reference: Cyber Bullying, Policy 4527
Code of Conduct, Policy 5300

Adopted: October 5, 2004

Revised: June 27, 2017; January 7, 2014

SOUTH COLONIE CENTRAL SCHOOL DISTRICT

Confidentiality and Security Agreement

First Name ________________________ Middle Initial ______ Last Name ______________________________

Home School/Building _____________________ Phone _____________ Job Title _________________________

Security and confidentiality records, reports, and files are matters of critical importance to the South Colonie Central School District (SCCSD). The purpose of this statement is to clarify your responsibilities as a privileged user of the SCCSD Information Technology Services (ITS). Each individual who has privileged access to sensitive, classified, or confidential data and privileged access to ITS configurations is expected to adhere to the security and confidentiality principles stated below.

As a person who has access to such information, you will not:

- share your password with any person, or permit any other person to access information under your account
- permit the unauthorized use of any information in documentation, configuration file, records, reports, and files which are accessed, processed, maintained, or stored by the Information Technology Department
- seek personal benefit from information that you have acquired as a result of your access to data
- disclose the confidential contents of any record, report, or file to any person, except in the conduct of official work assignments
- knowingly include a false, inaccurate, or misleading entry in any official no-test record, report, or file
- knowingly destroy data from any record, report, or file, except as authorized
- remove any documentation, configuration file, record, report, or file from the office where it is maintained, except in the performance of your official duties
- fail to comply with the legal restrictions regarding the use of information resources
- cause or assist another person to violate these principles

Violation of these principles may lead to disciplinary action consistent with applicable personnel policies. Violations may also lead to action under state and federal law pertaining to theft, alteration of public records, or other applicable sections.

Your signature below indicates that you have read, understand and will comply with these principles.

Employee Signature: ____ Date: __________________________

To Be Completed by the Supervisor of Information Technology

I have reviewed the request and authorize the individual indicated above to have access to specified systems.

IT Supervisor Name: ____ Date: ___________________

IT Supervisor Signature: ____

SOUTH COLONIE CENTRAL SCHOOL DISTRICT

Employee Account Agreement

First Name ________________________ Middle Initial ______ Last Name ______________________________

Home School/Building _____________________ Phone _____________ Job Title _________________________

In order to become a user of the South Colonie Central School District's telecommunication systems, technology resources, networks, e-mail and internet accounts, I hereby agree to comply with all District regulations for use of communication and technology as presently in force and as may be amended from time to time. I have read the *South Colonie Central School District Technology Use Policy & Regulations for Staff Members.* I agree to follow the rules contained in these documents. I understand that if I violate the rules, my account may be terminated and I may face other disciplinary action and/or prosecution.

Employee Initials ____________

In consideration for using the South Colonie Central School District's network resources and in consideration for having access to information contained on them, I hereby release the South Colonie Central School District, its personnel and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the system, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

As a user of South Colonie Central School District ITS, I agree not to:

- violate the property rights and copyrights in data and computer programs
- intentionally or neglectfully destroy or damage users' data or programs
- obtain unauthorized access to and use of an account and the networking facilities for purposes other than that intended
- obtain unauthorized access to and use an account and the networking facilities for personal or private gain
- read or use private files/data without proper authorization
- divulge the contents of any data base holding personnel and confidential information related to children, parents, or school business operations
- attempt, without authorization, to modify computer hardware or systems software
- use the network to send unsolicited, non-educationally related messages which consume system resources
- fraudulently use another person's name to send or receive messages
- fail to comply with the legal restrictions regarding the use of information resources
- use the system for any purpose that could be viewed as unprofessional

Your signature below indicates that you have read, understand and will comply with the principles outlines above.

Employee Signature: ____ Date: __________________________

SOUTH COLONIE CENTRAL SCHOOL DISTRICT

Network Access Request Form

PART I *(to be completed by employee)*

First Name ________________________ Middle Initial _______ Last Name ______________________________

Home School/Building _____________________ Phone _____________ Job Title ________________________

Employee Signature: ____ Date: ___________________________

- · - · - · - · - · - · - · - · - · - · - · - · - · - · - · - · -

PART II *(to be completed by Information Technology Supervisor)*

Use Login ____

Assigned Password ____ *(to be changed on first login)*

Completed by: ____ Date: ___________________________

- · - · - · - · - · - · - · - · - · - · - · - · - · - · - · - · -

Required Services: □ E-Mail □ Internet □ Student Information System

Return to ITD Help Desk at District Office

- · - · - · - · - · - · - · - · - · - · - · - · - · - · - · - · -

For Office Use Only

IT Supervisor Name: ____ Date: ____________________

IT Supervisor Signature: ____