Policies, Regulations and Forms Governing the Use of Technology

August 2022

Stafford Public Schools
Policies, Regulations and Forms
Governing the Use of Technology

Table of Contents

Stafford Public Schools
Office of the Superintendent of Schools
16 Levinthal Run
Stafford Springs, CT 06076
Tel. 860.684.2208 · Fax 860.684.5172
www.stafford.k12.ct.us

Steven A. Moccio
Superintendent of Schools

August 2022

Dear Parents/Guardians, Students and Staff:

The *Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology* (August 2021), is comprised of several Board of Education policies, regulations and forms. To make it easier to know which policies are relevant to role, the packet of information is broken into two sections, one for staff and the other for students. As the district has now instituted a 1:1 Device Program at each school, an additional policy has been included for students, along with updated device loan agreements for students and staff. As a reminder,

- The Acceptable Use Agreement, Internet and Network Specific Terms & Conditions for Use Forms must be signed annually. Please note that the forms are valid through October 1 of the subsequent school year. There are separate forms for each of the following:
  - Elementary Student & Parent/Guardian Agreement
  - Middle & High School Student and Parent/Guardian Agreement
  - Faculty and Staff [Agreement]
- Social Media Policy (#4118.51/4218.51) and Regulation were revised and should be reviewed annually by all staff.
- Use of Private Technology Devices by Students (#5131.84, formerly known as the Bring Your Own Device Policy) and Regulation have been revised. All students are required to use the district provided device and should not bring their personal devices.

It is necessary for parents/guardians/students age 18 or over, faculty and staff, to review the publication entitled, *Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology* (August 2021), which is posted on our website under "For Parents" and "For Staff", and sign the required forms each year. In addition to being posted on the district website, a hard copy of this publication can be requested in each school office. Please review the policies & regulations, complete and submit this online form **no later than Friday, September 10, 2021.**

Should you have any questions regarding the information contained in the policies or regulations, please contact your school office. Thank you, in advance, for your cooperation with this very important matter.

Sincerely,

Steven A. Moccio
Superintendent of Schools

4118.5 (a)
4218.5 (a)

Personnel -- Certified -- Non-Certified

Rights, Responsibilities and Duties

Employee Use of the District's Computer Systems and Electronic Communications

Computers, computer networks, electronic devices, Internet access, and e-mail are effective and important technological resources. The Stafford Board of Education (the "Board") has installed computers and a computer network, including Internet access and an e-mail system, on Board premises and may provide other electronic devices that can access the network such as wireless and/or portable electronic handheld equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. (including, but not limited to, personal laptops, Smartphones, network access devices, Kindles, Nooks, cellular telephones, radios, personal cassette players, CD players, iPads or other tablet computers, walkie-talkies, Blackberries, personal data assistants, iPhones, Androids and other electronic signaling devices). The Board's computers, computer networks, electronic devices, Internet access, and e-mail are referred to collectively as "the computer systems" and are provided in order to enhance both the educational opportunities for our students and the business operations of the district.

These computer systems are business and educational tools. As such, they are made available to Board employees for business and education-related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such computer systems are used for appropriate business and education-related purposes.

In accordance with applicable laws and the Administrative Regulations associated with this Policy, the system administrator and others managing the computer systems may access email or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including but not limited to, Twitter, Facebook, LinkedIn, and YouTube.

Incidental personal use of the computer systems may be permitted solely for the purpose of e-mail transmissions and access to the Internet on a limited, occasional basis. Such incidental personal use of the computer systems, however, is subject to all rules, including monitoring of all such use, as the Superintendent may establish through regulation. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities.

Users should not have any expectation of personal privacy in the use of the computer system or other electronic devices that access the computer system. Use of the computer system represents an employee's acknowledgement that the employee has read and understands this policy and any applicable regulations in their entirety, including the provisions regarding monitoring and review of computer activity.

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250
Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

Policy Adopted: January 30, 2017
Policy Revised: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

Personnel -- Certified -- Non-Certified

Rights, Responsibilities and Duties

Employee Use of the District's Computer Systems and Electronic Communications

Introduction

Computers, computer networks, electronic devices, Internet access, and electronic mail are effective and important technological resources. The Board of Education has installed computers and a computer network, including Internet access and an e-mail system, on Board premises and may provide electronic devices that can access the system, such as personal laptops, Smartphones, I-Pads or other tablet computers, I-Phones, Androids or other mobile or handheld electronic devices, to enhance the educational and business operations of the district. In these regulations, the computers, computer network, electronic devices, Internet access and e-mail system are referred to collectively as "the computer systems."

These computer systems are business and educational tools. As such, they are being made available to employees of the district for district-related educational and business purposes. *All users of the computer systems must restrict themselves to appropriate district-related educational and business purposes.* Incidental personal use of the computer systems may be permitted solely for the purpose of e-mail transmissions and similar communications, including access to the Internet on a limited, occasional basis. Such incidental personal use of the computer systems is subject to all rules, including monitoring of all such use, set out in these regulations. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities.

These computer systems are expensive to install, own and maintain. Unfortunately, these computer systems can be misused in a variety of ways, some of which are innocent and others deliberate. Therefore, in order to maximize the benefits of these technologies to the district, our employees and all our students, this regulation shall govern all use of these computer systems.

Monitoring

It is important for all users of these computer systems to understand that the Board of Education, as the owner of the computer systems, reserves the right to monitor the use of the computer systems to ensure that they are being used in accordance with these regulations. The Board of Education intends to monitor in a limited fashion, but will do so as needed to ensure that the systems are being used appropriately for district-related educational and business purposes and to maximize utilization of the systems for such business and educational purposes. The Superintendent reserves the right to eliminate personal use of the district's computer systems by any or all employees at any time.

The system administrator and others managing the computer systems may access email or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including, but not limited to, Twitter, Facebook, LinkedIn, and YouTube.

Notwithstanding the above and in accordance with state law, the Board may not: (1) request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing a personal online account; (2) request or require that an employee authenticate or access a personal online account in the presence of a Board representative; or (3) require that an employee invite a supervisor employed by the Board or accept an invitation from a supervisor employed by the Board to join a group affiliated with any personal online account of the employee. However, the Board may request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing (1) any account or service provided by Board or by virtue of the employee's employment relationship with the Board or that the employee uses for the Board's business purposes, or (2) any electronic communications device supplied or paid for, in whole or in part, by the Board.

In accordance with applicable law, the Board maintains the right to require an employee to allow the Board to access his or her personal online account, without disclosing the user name and password, password or other authentication means for accessing such personal online account, for the purpose of:

(A) Conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee's personal online account; or

(B) Conducting an investigation based on the receipt of specific information about an employee's unauthorized transfer of the Board's proprietary information, confidential information or financial data to or from a personal online account operated by an employee or other source.

For purposes of these Administrative Regulations, "personal online account" means any online account that is used by an employee exclusively for personal purposes and unrelated to any business purpose of the Board, including, but not limited to, electronic mail, social media and retail-based Internet web sites. "Personal online account" does not include any account created, maintained, used or accessed by an employee for a business purpose of the Board.

Why Monitor?

The computer systems are expensive for the Board to install, operate and maintain. For that reason alone it is necessary to prevent misuse of the computer systems. However, there are other equally important reasons why the Board intends to monitor the use of these computer systems, reasons that support its efforts to maintain a comfortable and pleasant work environment for all employees.

These computer systems can be used for improper, and even illegal, purposes. Experience by other operators of such computer systems has shown that they can be used for such wrongful purposes as sexual harassment, intimidation of co-workers, threatening of coworkers, breaches of confidentiality, copyright infringement and the like.

Monitoring will also allow the Board to continually reassess the utility of the computer systems, and whenever appropriate, make such changes to the computer systems as it deems fit. Thus, the Board monitoring should serve to increase the value of the system to the district on an ongoing basis.

Privacy Issues

Employees must understand that the Board has reserved the right to conduct monitoring of these computer systems and can do so despite the assignment to individual employees of passwords for system security. Any password systems implemented by the district are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user.

The system's security aspects, message delete function and personal passwords can be by-passed for monitoring purposes.

Therefore, employees must be aware that they should not have any expectation of personal privacy in the use of these computer systems. This provision applies to any and all uses of the district's computer systems and electronic devices that access same, including any incidental personal use permitted in accordance with these regulations.

Use of the computer system represents an employee 's acknowledgement that the employee has read and understands these regulations and any applicable policy in their entirety. including the provisions regarding monitoring and review of computer activity.

Prohibited Uses

Inappropriate use of district computer systems is expressly prohibited, including, but not limited to, the following:

- Sending any form of solicitation not directly related to the business of the Board of Education;
- Sending any form of slanderous, harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);

- Gaining or seeking to gain unauthorized access to computer systems;
- Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from supervisory personnel;
- Sending any message that breaches the Board of Education's confidentiality requirements, including the confidentiality rights of students;
- Sending any copyrighted material over the system;
- Sending messages for any purpose prohibited by law;
- Transmission or receipt of inappropriate e-mail communications or accessing inappropriate information on the Internet, including vulgar, lewd or obscene words or pictures;
- Using computer systems for any purposes, or in any manner, other than those permitted under these regulations;
- Using social networking sites such as Facebook, Twitter, LinkedIn and YouTube in a manner that violates the Board's Social Networking policy.

In addition, if a particular behavior or activity is generally prohibited by law and/or Board of Education policy, use of these computer systems for the purpose of carrying out such activity and/or behavior is also prohibited.

Electronic Communications

The Board expects that all employees will comply with all applicable Board policies and standards of professional conduct when engaging in any form of electronic communication, including texting, using the district's computer system, or through the use of any electronic device or mobile device owned, leased, or used by the Board. As with any form of communication, the Board expects district personnel to exercise caution and appropriate judgment when using electronic communications with students, colleagues and other individuals in the context of fulfilling an employee's job-related responsibilities, including when engaging in remote teaching or use of a digital teaching platform.

Your school email must contain a signature and must include a confidentiality statement. "This message has been sent to you from the (title) of Stafford (name of school) School and contains information which is confidential and/or privileged. If you are not the intended recipient, please advise the sender immediately by reply e-mail and delete this message and any attachments without retaining a copy. Thank you."

Websites

The Board allows the central office and schools within the district to create and maintain web sites for educational and informational purposes.

District and individual school web sites shall be used to share information about school curriculum and instruction, school-authorized activities, and other information relating to our schools and our mission. Web sites shall also provide instructional resources for staff and students.

Disciplinary Action

Misuse of these computer systems will not be tolerated and will result in disciplinary action up to and including termination of employment. Because no two situations are identical, the Board reserves the right to determine the appropriate discipline for any particular set of circumstances.

Complaints of Problems or Misuse

Anyone who is aware of problems with or misuse of these computer systems, or has a question regarding the appropriate use of the computer systems, should report this to his or her supervisor or to the District IT / Network Coordinator.

Most importantly, the Board urges *any* employee who receives *any* harassing, threatening, intimidating or other improper message through the computer systems to report this immediately. It is the Board's policy that no employee should be required to tolerate such treatment, regardless of the identity of the sender of the message. *Please report these events!*

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250
Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

Regulation adopted: January 30, 2017
Regulation reviewed: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

NOTICE REGARDING ELECTRONIC MONITORING

[To be posted in a conspicuous place readily available for viewing by employees]

In accordance with the provisions of Connecticut General Statutes Section 31-48d, the Board of Education hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the Board may not actually engage in the use of electronic monitoring, it reserves the right to do so as the Board and/or the Administration deem appropriate in their discretion, consistent with the provisions set forth in this Notice.

"Electronic monitoring," as defined by Connecticut General Statutes Section 31-48d, means the collection of information on the Board's premises concerning employees' activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the Board's premises which are open to the public, or (B) which is prohibited under other state or federal law.

The following specific types of electronic monitoring may be used by the Board in its workplaces:

- Monitoring of e-mail and other components of the Board's computer systems, including monitoring of electronic devices such as PDAs, Smartphones, and mobile or handheld devices that access the computer systems, for compliance with the Board's policies and regulations concerning use of such systems.

- Video and/or audio surveillance within school buildings (other than in restrooms, locker rooms, lounges and other areas designed for the health or personal comfort of employees or for the safeguarding of their possessions), on school grounds and on school buses and other vehicles providing transportation to students and/or employees of the school system.

- Monitoring of employee usage of the school district's telephone systems.

The law also provides that, where electronic monitoring may produce evidence of misconduct, the Board may use electronic monitoring without any prior notice when the Board has reasonable grounds to believe employees are engaged in conduct that (i) violates the law, (ii) violates the legal rights of the Board or other employees, or (iii) creates a hostile work environment.

Questions about electronic monitoring in the workplace should be directed to the Superintendent.

4118.5 REG
4218.5 REG
Form 1 (a)

Stafford Public Schools
Acceptable Use Agreement
Internet and Network
Specific Terms and Conditions for Users

(Faculty and Staff)

Please sign and return the last page of this agreement to the building principal/your supervisor.

The Stafford School District provides an array of technology resources for faculty and staff use to enhance the learning environment, facilitate resource sharing, and to promote communication. This agreement outlines appropriate use and prohibited activities when using technology resources. Every faculty and staff member is expected to follow all guidelines listed below, as well as those given verbally by your principal or supervisor, and to demonstrate good citizenship and ethical behavior at all times.

In accepting this agreement, faculty and staff acknowledge the following rules and conditions:

Government Laws

I will use computers in conformity with laws of the United States and the State of Connecticut. Violations include, but are not limited to, the following:

Criminal Acts – These include, but are not limited to, "hacking" or attempting to access computer systems without authorization, harassing email, cyber bullying, cyber stalking, child pornography, vandalism, and/or unauthorized tampering with computer systems.

Libel Laws - Publicly defaming people through the published material on the Internet, email, and social media.

Copyright Violations - Copying, selling, showing, changing or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), engaging in plagiarism (using others' words or ideas as your own). An employee shall not use the District's logo or other copyrighted material of the District without express, written consent.

Netiquette and Appropriate Use Guidelines

Network Resources - The use of the network is a privilege, not a right, and may be revoked if abused. Faculty/staff are personally responsible for his/her actions when utilizing the school 's computer resources.

Privacy – Network storage areas are the property of the school District. The Network Administrator may review any storage area of the school network or email to maintain system integrity and to ensure that faculty/staff are using the system responsibly. No one can claim a right to privacy or unrestricted speech in the use of the District's systems.

Personal Use - Limited personal use is permitted as long as this does not increase the cost to the District or interfere with the operations of the network or with the performance of the employee's duties. Use of the District's digital resources at home can become a potential risk for viruses and spyware being introduced into the school network. Please use extreme caution when using district resources at home.

Copying/Downloading - Faculty/Staff are NOT permitted to download or install any software, shareware, or freeware onto the school's computers. Faculty/Staff are NOT permitted to intrude into other faculty/staff files.

Inappropriate Materials Or Language – Faculty/Staff are NOT permitted to transmit, retrieve or store materials that are discriminatory, harassing, obscene, pornographic, or inappropriate. Despite our best efforts and beyond the limits of filtering technology, you may run across areas of adult content and some material you might find objectionable for the educational setting. We ask that you report these websites to the technology department to include in the filtering process. Faculty or staff should not seek to access sites that are inappropriate for the public school environment. The use of District online systems for personal gain, political lobbying or any other purpose which is illegal or against District policy or contrary to the District's best interest is NOT permitted.

Electronic Mail – While electronic mail can be a valuable tool, it is impossible to guarantee that it will be private. Do not send messages that are abusive, threatening, harassing, obscene, sexually oriented, discriminatory, damaging, illegal, false, or contain profanity. Do not send chain letters, virus warnings, urban legends or other unsubstantiated scares. Use the forward button with care (copy/paste is preferred). Do not use the system for commercial purposes, financial gain, political lobbying or any illegal purposes. Faculty/Staff can be permitted to send messages pertaining to SCHOOL SPONSORED events, only after checking with appropriate District/campus technology personnel or your direct supervisor. Do not open attachments without first checking the validity of the attachment with the sender. If the sender is unknown, don't open the attachment.

Social Media Guidelines – Refer to Social Media Policy and corresponding Regulations (#4118.51/4218.51).

Faculty/Staff Understanding

- I understand that passwords are private. I will not allow others to use my account name and password, or try to use that of others. I understand that my school network and email accounts are owned by the District and are not private. Stafford School District has the right to access my information at any time.
- I understand that only students with proper authorization should be allowed to access the network or Internet.
- I understand that all student use of the Internet is to be supervised.
- I will check that any personal storage devices used not contain malware or viruses and also check for inappropriate content before using it on school equipment.
- I will be polite and use appropriate language in my email messages, virtual learning environments, online postings, and other digital communications with

others. I will refrain from using profanity, vulgarities or any other inappropriate language.

- I will use email and other means of digital communications responsibly. I will not use digital devices or the Internet to send or post hate or harassing mail, pornography, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors either at school or at home.
- I understand that my online activities can reflect on the school district. I understand that what I do on social networking websites should not reflect negatively on my fellow teachers, staff, students, or on the school district. I understand that I will be held responsible for how I represent myself and my school, department or district on the Internet.
- I understand that masquerading, spoofing, or pretending to be someone else is forbidden. This includes, but is not limited to, sending out e-mail, creating accounts, or posting messages or other online content in someone else's name.
- I will use technology resources responsibly. I will not retrieve, save, or display hate-based, offensive or sexually explicit material using any of Stafford Public School 's computer resources. I am responsible for not pursuing material that could be considered offensive. I understand that I am to notify the technology department immediately if by accident I encounter materials which violate appropriate use.
- I will use technology resources productively and responsibly for school-related purposes. I will avoid using any technology resource in such a way that would disrupt the activities of other users. This includes intentionally wasting resources, downloading music or videos for personal use, playing online games, creating or printing inappropriate materials, printing excessive quantities, tampering with computer parts, erasing programs or others' files, introducing viruses, hacking, attempting to gain unauthorized access and modifying settings without permission.
- I will refrain from attempting to bypass or circumvent security settings or Internet filters, or interfering with the operation of the network by installing illegal software, web-based services and/or software not approved by the Stafford Technology Department.
- I understand that vandalism is prohibited. This includes but is not limited to modifying or destroying equipment, programs, files, or settings on any computer or other technology resource.
- I will respect the intellectual property of other users and information providers. I will obey copyright guidelines. I will not plagiarize or use other's work without proper citation and permission.
- I will refrain from the use of or access of files, software, or other resources owned by others. I will use only those school network folders that are designated for my use or for the purpose designated by my principal/supervisor.
- I will follow all guidelines set forth by the District when publishing schoolwork online (e.g. to a website, blog, wiki, discussion board, podcasting or video server).

- I understand the Internet is a source for information that is both true and false; and that the school is not responsible for inaccurate information obtained from the Internet. I agree to abide by all Internet safety guidelines that are provided by the school and to attend staff development related to Internet safety.
- I will ask for permission before connecting my own devices to the school's network unless it is on the district's approved list
- I understand that the school district is not responsible for any personal devices I may bring to school and I am solely responsible for my personal devices including equipment that is lost, stolen, or damaged.
- I also understand that district/campus technology personnel are not allowed to work on personal electronic devices.
- I understand that District administrators will deem what conduct is inappropriate use if such conduct is not specified in this agreement.

4118.5 REG
4218.5 REG
Form 1 (e)

ALL FACULTY/STAFF ARE REQUIRED TO SIGN AND RETURN THE APPLICATION FOR NETWORK ACCESS BEFORE THE USE OF ANY TECHNOLOGY EQUIPMENT (PERSONAL OR DISTRICT-OWNED) IS ALLOWED AT STAFFORD PUBLIC SCHOOLS.

Faculty/Staff Agreement:

As a user of the school's technology resources, I understand and agree to comply with the specific terms and conditions for users as outlined in this Acceptable Use Agreement for Faculty/Staff. I also understand that I am responsible for reading and following all of the Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology.

I understand the conditions for use of the network and Internet resources provided by the Stafford School District and that access to technology resources are provided for the purpose of promoting educational excellence in keeping with the academic goals of the District, and that faculty/staff use for any other purpose is inappropriate. I recognize it is impossible for the District to restrict access to all controversial materials, and I will not hold the school responsible for materials acquired on the school network.

Consequences for Violation Of This Agreement

I understand that I am responsible for any transactions that occur under my user ID or account. Should I commit a violation, I understand that consequences of my actions could include suspension of access to the system, loss of computer privileges or data and files, revocation of the computer system account, disciplinary action, and/or referral to law enforcement.

Faculty/Staff Name (print): _____

Faculty/Staff Signature: _____ Date: _____

New Stafford Employee Password* :

_____

*Your password must be a minimum of eight (8) characters and must be alphanumeric. Including special characters (such as $, %, or *) is recommended.

An employee's user name will be the employee's last name and first initial, with letters added from the first name to make the user name unique (if necessary).

Please sign and return this page of this agreement to the building principal/your supervisor, as directed.

4118.5 (a) REG
4218.5 (a) REG
Form 2

Stafford Public Schools
Staff Device Loan Agreement

Responsibilities

By signing the *Stafford Public Schools Acceptable Use Agreement and Application for Network Access*, staff have agreed to follow the guidelines contained within it, and all local, state, and federal laws. Any violation of any of these policies may result in a loss of network privileges, loss of right to use the device, and / or discipline.

The use of district issued technology is a privilege and intended for school purposes only. By accepting a district issued device the following conditions shall apply:

- Suspicious links will be avoided, and the manufacturer's operating system will not be replaced with custom software (i.e. "jailbreaking" the device).
- All accounts and/or passwords will be kept secure and will not be shared with other individuals. This includes passwords for email and / or network access.
- Email and other computer communication media should only be used for appropriate, legitimate, and responsible communication.
- Stafford Public Schools is not responsible for loss of data. It is the user's responsibility to store and backup files.
- Only district staff are authorized to repair a district issued device.
- Stafford Public Schools personnel have remote access to the device and/or files, and are allowed to utilize this access at any time should an issue arise.

Proper Care

Proper care of the district issued device is required. Guidelines for proper care are listed below.

- The device should be kept in a secure location at all times.
- The device should never be dropped.
- The device should never be left in places of extreme hot or cold temperatures, humidity, or limited ventilation for an extended period of time.
- The device should only be cleaned with a soft cloth.
- Eating or drinking when using the device should be avoided.
- Defacing the device in any manner is prohibited (including the addition of stickers and labels).

4118.5 (b) REG
4218.5 (b) REG
Form 2

Acknowledgement

Staff members agree to abide by the *Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology*, as were provided at the beginning of the school year (copy available at www.stafford.k12.ct.us, under "For Staff") and shall follow the principles of good digital citizenship.

By signing this Agreement below, staff members acknowledge the following:

- ✓ I have read, understand, and agree to the terms and conditions outlined in this Agreement.
- ✓ I understand that the condition of this device will be documented upon distribution. I further understand that I am financially responsible for loss or damage due to neglect and will be required to reimburse the district, up to full replacement cost.
- ✓ I agree to return the district issued device and any accessories provided by the district, when requested to do so or at the time of withdrawal from the Stafford Public Schools, whichever comes first.

Signature of Staff Member: _____ Date: _____

Printed Name: _____ Asset Tag #: _____

Staff should return this form to the school office.

4118.51
4218.51

Personnel-Certified / Non Certified

Social Media

The Stafford Board of Education (the "Board") recognizes the importance and utility of social media and networks for its employees. The laws regarding social media continue to evolve and change. Nothing in this policy is intended to limit an employee's right to use social media or personal online accounts under applicable law, as it may evolve. The Board acknowledges, for example, that its employees have the right under the First Amendment, in certain circumstances, to speak out on matters of public concern. The Board will resolve any conflict between this policy and applicable law in favor of the law.

Ordinarily, the use of social media by employees, including employees' use of personal online accounts, will not be a legal or policy issue. While a policy cannot address every instance of inappropriate social media use, employees must refrain from social media use that:

1) interferes, disrupts or undermines the effective operation of the school district;
2) is used to engage in harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate communications;
3) creates a hostile work environment;
4) breaches confidentiality obligations of school district employees; or
5) violates the law, board policies and/or other school rules and regulations.

The Board of Education, through its Superintendent, will adopt and maintain administrative regulations to implement this policy.

Legal References:

U.S. Constitution, Amend. I
Conn. Constitution, Article I, Sections 3, 4, 14
Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520
Conn. Gen. Stat. 31-40x
Conn. Gen. Stat. 31-48d
Conn. Gen. Stat. § 31-51q
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250

Policy adopted: January 30, 2017
Policy revised: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

4118.51 (a) REG
4218.51 (a) REG

Personnel-Certified / Non Certified

Social Media

The Stafford Board of Education (the "Board") recognizes the importance and utility of social media and networks for its employees. The laws regarding social media continue to evolve and change. Nothing in the Board's policy or these administrative regulations is intended to limit an employee's right to use social media or personal online accounts under applicable law, as it may evolve. The Board acknowledges, for example, that its employees have the right under the First Amendment, in certain circumstances, to speak out on matters of public concern. The Board will resolve any conflict between the Board's policy or these regulations and applicable law in favor of the law.
Ordinarily, the use of social media by employees, including employees' personal online accounts, will not be a legal or policy issue. While a policy or regulation cannot address every instance of inappropriate social media use, employees must refrain from social media use that:

1) interferes, disrupts or undermines the effective operation of the school district;
2) is used to engage in harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate communications;
3) creates a hostile work environment;
4) breaches confidentiality obligations of school district employees; or
5) violates the law, Board policies and/or other school rules and regulations.

Definitions:

The rapid speed at which technology continuously evolves makes it difficult, if not impossible, to identify all types of social media.

Thus, the term Social Media includes a variety of online tools and services that allow users to publish content and interact with their audiences. By way of example, social media includes, but is not limited to, the following websites or applications, including an employee's personal online account using such social media:

(1) social-networking (e.g. Facebook, Linkedln, Google+, Classmates.com);
(2) blogs and micro-blogs (e.g. Twitter, Tumblr, Medium);
(3) content-sharing (e.g. Scribd, SlideShare, DropBox);
(4) image sharing, video sharing or livestreaming (e.g. Snapchat, Periscope, Flickr, YouTube, Instagram, Vine, Pinterest);
(5) other sharing sites or apps such as by sound, location, news, or messaging, etc. (e.g. Reddit, Kik, Yik Yak, SoundCloud, WhatsApp).

Board of Education includes all names, logos, buildings, images and entities under the authority of the Board of Education.

Electronic communications device includes any electronic device that is capable of transmitting, accepting or processing data, including, but not limited to, a computer, computer network and computer system, and a cellular or wireless telephone.

Personal online account includes any online account that is used by an employee exclusively for personal purposes and unrelated to any business purpose of the Board, including, but not limited to electronic mail, social media and retail-based Internet websites. Personal online account does not include any account created, maintained, used or accessed by an employee for a business, educational or instructional purpose of the Board.

Rules Concerning District-Sponsored Social Media Activity

1. In order for an employee to use social media sites as an educational tool or in relation to extracurricular activities or programs of the school district, the employee must seek and obtain the prior permission of his/her supervisor.

2. Employees may not use personal online accounts to access social media for classroom activities without express permission of the employee's supervisor. Where appropriate and with permission, district-sponsored social media accounts should be used for such purposes.

3. If an employee wishes to use social media sites to communicate meetings, activities, games, responsibilities, announcements etc., for a school-based club or a school-based activity or an official school-based organization, or an official sports team, the employee must also comply with the following rules:
    - The employee must receive the permission of his/her immediate supervisor.
    - The employee must not use his/her personal online account for such purpose, but shall use his/her Board-issued account.
    - The employee must ensure that such social media use is compliant with all Board of Education policies, regulations, and applicable state and federal law, including the provision of required legal notices and permission slips to parents.
    - The employee must set up the club, etc. as a group list which will be "closed" (e.g. membership in the group is limited to students, parents and appropriate school personnel), and "monitored" (e.g. the employee had the ability to access and supervise communications on the social media site).
    - Parents shall be permitted to access any page that their child has been invited to join.
    - Access to the page may only be permitted for educational purposes related to the club, activity, organization or team.
    - The employee responsible for the page will monitor it regularly.
    - The employee's supervisor shall be permitted access to any page established by the employee for a school-related purpose.

- Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all such district-sponsored social media activity.

4. Employees are prohibited from making harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate statements in their social media communications using district-sponsored sites or accounts or through Board-issued electronic accounts.

5. Employees are required to comply with all Board of Education policies and procedures and all applicable laws with respect to the use of electronic communications devices, networks, Board-issued accounts, or when accessing district-sponsored social media sites or while using personal devices on the district's wireless network or while accessing district servers.

6. The Board of Education reserves the right to monitor all employee use of district computers and other electronic devices, including employee blogging and social networking activity. An employee should have no expectation of personal privacy in any communication made through social media, including personal online accounts, while using district electronic communications devices.

7. All communications through district-sponsored social media or Board-issued electronic accounts must comply with the Board of Education's policies concerning confidentiality, including the confidentiality of student information. If an employee is considering sharing information and is unsure about the confidential nature of the information, the employee shall consult with his/her supervisor prior to communicating such information.

8. An employee may not link a district-sponsored social media page to any personal online account or sites not sponsored by the school district.

9. An employee may not use district-sponsored social media or Board-issued electronic accounts for communications for private financial gain, political, commercial, advertisement, proselytizing or solicitation purposes.

10. An employee may not use district-sponsored social media or Board-issued electronic accounts in a manner that misrepresents personal views as those of the Board of Education, individual school or school district, or in a manner that could be construed as such.

Rules Concerning Personal Online Accounts

1. The Board understands that employees utilize social media and the web for personal matters in the workplace. The Board of Education reserves the right to monitor all employee use of district electronic communications devices, including a review of online and personal social media activities. An employee should have no expectation of personal privacy in any personal communication made through social media while using district computers, district-issued cellular telephones or other electronic communications devices.

While the Board reserves the right to monitor use of its electronic communications devices, employees may engage in incidental personal use of social media in the workplace so long as such use does not interfere with operations and productivity, and does not violate other Board policies.

2. An employee may not mention, discuss, reference or link to the Board of Education, the school district or its individual schools, programs or teams using personal online accounts or other sites or applications in a manner that could reasonably be construed as an official school district communication, unless the employee also states within the communication that such communication is the personal view of the employee of the school district and that the views expressed are the employee's alone and do not represent the views of the school district or the Board of Education. An example of such a disclaimer is: "the opinions and views expressed are those of the author and do not necessarily represent the position or opinion of the school district or Board of Education." For example, except as may be permitted by Board policy, employees may not provide job references for other individuals on social media that indicate that such references are made in an official capacity on behalf of the Board of Education.

3. Employees are required to maintain appropriate professional boundaries with students, parents, and colleagues. For example, absent an unrelated online relationship (e.g., relative, family friend, or personal friendship unrelated to school), it is not appropriate for a teacher or administrator to "friend" a student or his/her parent or guardian or otherwise establish special relationships with selected students through personal online accounts, and it is not appropriate for an employee to give students or parents access to personal postings unrelated to school.

4. In accordance with the public trust doctrine, employees are advised to refrain from engaging in harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate communications through personal online accounts. Such communications reflect poorly on the school district's reputation, can affect the educational process and may substantially and materially interfere with an employee's ability to fulfill his/her professional responsibilities.

5. Employees are individually responsible for their personal communications through social media and personal online accounts. Employees may be sued by other employees, parents or others, and any individual that views an employee's communication through social media and personal online accounts as defamatory, pornographic, proprietary, harassing, libelous or creating a hostile work environment. In addition, employees should consider refraining from posting anything that belongs to another person or entity, such as copyrighted publications or trademarked images. As all of these activities are outside the scope of employment, employees may be personally liable for such claims.

6. Employees are required to comply with all Board of Education policies and procedures with respect to the use of electronic communications devices when accessing personal online accounts and/or social media through district computer systems. Any access to personal online accounts and/or personal social media activities while on school property

or using school district equipment must comply with those policies, and may not interfere with an employee's duties at work.

7. All communications through personal online accounts and/or social media must comply with the Board of Education's policies concerning confidentiality, including the confidentiality of student information. If an employee is considering sharing information and is unsure about the confidential nature of the information, the employee shall consult with his/her supervisor prior to communicating such information.

8. An employee may not post official Board of Education material using a personal online account without written permission of his/her supervisor.

9. All of the Board of Education's policies and administrative regulations apply to employee use of personal online accounts in the same way that they apply to conduct that occurs in the workplace and off duty conduct.

Access to Personal Online Accounts

1. An employee may not be required by his/her supervisor to provide his/her username, password, or other means of authentication of a personal online account.

2. An employee may not be required to authenticate or access a personal online account in the presence of his/her supervisor.

3. An employee may not be required to invite or accept an invitation from his/her supervisor or required to join a group with the employee's personal online account.

Use of Crowdfunding Activities

Prior to engaging in any crowdfunding activities (e.g. DonorsChoose, Kickstarter, GoFundMe, etc) for the Board of Education, its schools, classes, or extracurricular teams or clubs, an employee must first apply in writing to the building principal and receive approval for the crowdfunding activity. Such written application must include the name of the website or application to be utilized, a full description of the reason for the crowdfunding activity, a copy of the proposed personal profile to be listed on the site/application, and the proposed content to be uploaded to the crowdfunding website or application, including images. Any money received from crowdfunding activities must be deposited directly into a school activity fund and may not first be received by the employee. Crowdfunding activities must comply with all Board of Education policies,
regulations and procedures, and shall not include photos of students or the sharing of any confidential student information.

Disciplinary Consequences

Violation of the Board's policy concerning the use of social media or these administrative regulations may lead to discipline up to and including the termination of employment consistent with state and federal law.

An employee may face disciplinary action up to and including termination of employment if an employee transmits, without the Board's permission, confidential information to or from the employee's personal online account.

An employee may not be disciplined for failing to provide his/her username, password, or other authentication means for accessing a personal online account, failing to authenticate or access a personal online account in the presence of his/her supervisor or failing to invite his/her supervisor or refusing to accept an invitation sent by his/her supervisor to join a group affiliated with a personal online account, except as provided herein.

Notwithstanding, the Board may require that an employee provide his/her username, password or other means of accessing or authenticating a personal online account for purposes of accessing any account or service provided by the Board for business purposes or any electronic communications device supplied by or paid for, in whole or in part, by the Board.

Nothing in this policy or regulations shall prevent the district from conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about an activity on an employee's personal online account or based on specific information about the transfer of confidential information to or from an employee's personal online account. During the course of such investigation, the district may require an employee to allow the district to access his or her personal online account for the purpose of conducting such investigation. However, the employee will not be required to provide his/her username and/or password or other authentication means in order for the district to access the personal online account.

Legal References:

U.S. Constitution, Amend. I
Conn. Constitution, Article I, Sections 3, 4, 14
Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520
Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. § 31-51q
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250

Regulation adopted: January 30, 2017
Regulation reviewed: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

Students

Student Use of the District's Computer Systems and Internet Safety

Computers, computer networks, electronic devices, Internet access, and e-mail are effective and important technological resources. The Stafford Board of Education (the "Board") has installed computers and a computer network, including Internet access and an e-mail system, on Board premises and may provide other electronic devices that can access the network such as wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing etc. (including, but not limited to, laptops, Kindles, radios, I-Pads, Chromebooks or other tablet computers). The Board's computers, computer network, electronic devices, Internet access, and e-mail are referred to collectively as "the computer systems" and are provided in order to enhance both the educational opportunities for our students and the business operations of the district.

These computer systems are business and educational tools. As such, they are made available to students in the district for education-related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such computer systems are used by students solely for education-related purposes. The Board will educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Additionally, the Board will implement a technology protection measure to block or filter Internet access to visual depictions that contain material, that is obscene or obscene as to minors or contains child pornography, and ensure that such filtering technology is operative during computer use by minor students to the extent practicable when such students are using Board-owned computers or devices and Board-provided Internet access.

As the owner of the computer systems, the Board reserves the right to monitor the use of the district's computers and computer systems.

Legal References:

Conn. Gen. Stat. § 10-221

Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. §§ 2510 through 2520

Children's Internet Protection Act, Pub. L. 106-554, codified at 47 U.S.C. § 254(h)

No Child Left Behind Act of 2001, Pub. L. 107-110, codified at 20 U.S.C. § 6777

Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 U.S.C. § 254(h)(5)(B)(iii)

Policy adopted: January 30, 2017
Policy revised: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

Students

Student Use of the District's Computer Systems and Internet Safety

1. Introduction

    a. Access to District Computer Systems When Students are Physically Present on School Property

When students are physically present on school property, the Board is pleased to offer students access to the district's computers and computer networks, including access to electronic mail (e-mail) and the Internet, as well as electronic devices, (all of which will be referred to collectively as "computer systems"). Access to the school's computer systems will enable students to explore libraries, databases, websites, and bulletin boards (e.g. blogs, discussion boards, digital classroom, etc.) while exchanging information with others. Such access is provided solely for education-related purposes. Use of the district's computer systems will be allowed only for students who act in a considerate and responsible manner in using such systems.

The Board of Education and the Administration believe in the educational value of such computer systems and recognize their potential to support our curriculum by expanding resources available for staff and student use. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

These computer systems are expensive to purchase, install and maintain. As the property of the district these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, students are required to adhere to a set of policies and procedures, as set forth in detail below, in conjunction with their use of the computer systems. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board's student discipline policy.

    b. Access to District Computer Systems When Students are Engaged in Remote Learning

The Board and the Administration recognize that technology is integral to the delivery of instruction if and when the district implements any form of digital or remote learning. The district may therefore provide students with remote access to some or all of the district's computer systems so that students may access the district's virtual learning environment. Such access, if granted, is provided solely for education-related purposes. Use of the district's computer systems will be allowed only for students who comply with district policies and procedures concerning computer system use, and demonstrate the ability to use the computer systems in a considerate and responsible manner.

These computer systems are expensive to purchase, install and maintain. As the property of the district, these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, students will be required to adhere to a set of policies and procedures, as set forth in detail below, in conjunction with their use of the computer systems. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board's student discipline policy.

Stafford Public Schools
Acceptable Use Agreement
Internet and Network
Specific Terms and Conditions for Users

(Elementary Student and Parent/Guardian Agreement)

The Stafford School District offers students access to computers and the Internet to support the district's vision and mission. In order to provide open access to the resources, tools, and equipment the school district believes is essential to teaching and learning, it is important that users understand their responsibilities and conduct themselves as good citizens and responsible learners at all times. Listed below are guidelines that outline responsible use.

I will:

- Keep private information private. (My password and identity are mine and not to be shared.)
- Treat others with respect both online and offline.
- Report to a teacher or other adult anyone who tries to use the computer to hurt or harass me or others.
- Work hard to be a responsible digital citizen.
- Encourage others to be good digital citizens.
- Have appropriate conversations in all my interactions with others.
- Tell adults when someone makes me feel uncomfortable.
- Use computers for school-related purposes.
- Credit my sources when I use others' information, images or other material.
- Respect the work of other students and not try to copy, damage, or delete their work.
- Follow District policies, rules, and regulations.
- Ask for permission before connecting my own devices to the school's network unless it is on the district's approved list.
- Take care of the District's computer equipment.

I will not:

- Read other student's private communications without permission.
- Use improper language or pictures.
- Use communication tools to spread lies about others.
- Pretend to be someone else online.
- Give out my full name, password, address or any other personal information to someone I don't know.
- Give out the full names and addresses of others.
- Use anyone's password other than my own or the one my teacher gives me.
- Send e-mail to anyone who asks me not to send them email.

- Talk to strangers in online conversations.
- Look for, read, view, or copy inappropriate pictures or information.

- Try to get access to or make the computer or network do things not approved by my school and the District.

I understand:

- That the computers, network and printers may not work every day.
- That sometimes my computer work may be lost, and I should be careful to back up important work.
- That some things I read on the Internet may not be true.
- That I may encounter inappropriate material by accident while using the Internet, and I should report it to my teacher or an adult immediately.
- That the computers and network belong to the District and that using them is a privilege, not a right.
- That it is my responsibility to make sure that any devices I use on a school network are approved.
- That the things that I do using a school computer or network are not private and that my teachers and District staff may review my work and activities at any time.

DISCLAIMER AND LIMITATION OF LIABILITY

Use of the Internet is provided on an "as is, as available" basis. You agree that this limitation is intended to, and does release Stafford Public Schools, its board of trustees, agents, and staff members from any claims, damages, or losses that you may suffer that may arise out of the use of this system.

Internet activities at the elementary level will be "teacher monitored". This policy, however, should apply anytime children are allowed to use a computer at school or observe someone using a computer at school. The same guidelines set forth in this policy will encourage proper usage at home. All children should be made aware that some materials are not suitable, and such material should always be reported to an adult.

After reading, please complete and sign the Application for Network Access and return it to your child's school office. Please keep this portion for future reference.

STAFFORD PUBLIC SCHOOLS APPLICATION FOR NETWORK ACCESS
(This form should be completed by a parent / guardian. Please print.)

Student's Full Name: _____
Home Address: _____
Home Phone: _____
School: _____
Homeroom Teacher: _____
Grade: (Please check one)
☐ Pre-Kindergarten ☐ Kindergarten ☐ 1st Grade ☐ 2nd Grade ☐ 3rd Grade ☐ 4th Grade ☐ 5th Grade

By signing below, I certify that all the information that I have provided on this form is correct and that I, as the Parent or Legal Guardian of the above named child, acknowledge and agree to the following:

- I have read and discussed this Acceptable Use Agreement with my child. I also understand that this agreement will be valid through October 1 of the following school year.
- I fully understand that this access is designed for educational purposes in keeping with the academic goals of the district, and that student use for any other purpose is inappropriate.
- I recognize that while every effort will be made to filter out controversial material, it is impossible for the Stafford School District to restrict access to all controversial material, and I will not hold Stafford Public Schools responsible for controversial material offered on the network.
- I understand that my child is responsible for any transactions that occur under his or her user ID or account whether it be on or off campus and that any violation of the Stafford Public Schools Policies, Regulations and Forms Governng the Use of Technology may result in my child being denied access to the district's technology resources, in addition to other disciplinary action.
- I understand that my child will use the Stafford Public Schools Network and have Internet access. I also understand the school could be publishing examples of my child's projects or publish photographs/video of my child participating in school related activities in district media or share with local media outlets. Unless otherwise notified in writing by a parent or guardian, the school will assume permission is given to publish students' names, work, videos, and photographs.

Parent or Guardian Signature: _____

Parent or Guardian Printed Name: _____

Parent or Guardian Address: _____

Parent or Guardian Phone Number: _____

Parent or Guardian Email Address: _____

Date: _____ School Year: _____

5131.83 REG
Form 1b

Stafford Public Schools
Acceptable Use Agreement
Internet and Network
Specific Terms and Conditions for Users

(Middle and High School Student and Parent/Guardian Agreement)

The Stafford School District provides an array of technology resources for student use. This agreement outlines appropriate use and prohibited activities when using technology resources. Every student is expected to follow all guidelines stated below, as well as those given orally by the staff, and to demonstrate good citizenship and ethical behavior at all times.

In accepting this agreement, students acknowledge the following rules and conditions:

Government Laws

I will use computers in conformity with laws of the United States of America and the State of Connecticut.

Violations include, but are not limited to, the following:

Criminal Acts – These include, but are not limited to, "hacking" or attempting to access computer systems without authorization, sending harassing email, cyber-bullying, cyber-stalking, accessing/distributing child pornography, vandalism, and/or unauthorized tampering with computer systems.

Libel Laws – Publicly defaming people through the published material on the Internet and/or email.

Copyright Violations – Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all material available on the Internet are protected by copyright), engaging in plagiarism (using other's words or ideas as your own).

Netiquette and Appropriate Use Guidelines:

Network Resources – The use of the school network is a privilege, not a right, and may be revoked if abused. The student is personally responsible for his/her actions when utilizing the school's computer resources. Despite our best efforts and beyond the limits of filtering technology, your child may run across areas of adult content and some material you might find objectionable.

Privacy – Network storage areas are the property of the school district. The Network Administrator may review any storage area of the school network to maintain system integrity and to ensure that students are using the system responsibly.

Copying/Downloading – Students are NOT permitted to download or install any software, shareware, or freeware onto the school 's computers. Students are NOT permitted to copy others' work or intrude into others' folders.

Inappropriate Materials or Language – Students are NOT permitted to transmit, retrieve or store materials that are discriminatory, harassing, obscene, pornographic, or inappropriate. Should students encounter such material by accident, they should report it to their teacher immediately. The use of District online systems for personal gain, political lobbying or any other purpose which is illegal or against District policy or contrary to the District's best interest is NOT permitted.

Student Understanding

- I understand that passwords are private. I will not allow others to use my account name and password, or try to use that of others. I understand that my school network and email accounts are owned by the District and are not private. Stafford Public Schools has the right to access my information at any time.
- I will be polite and use appropriate language in my digital communications with others. I will refrain from using profanity, vulgarities or any other inappropriate language as determined by school administrators.
- I will use email and technology resources (e.g. blogs, wikis, podcasting, chat, instant-messaging, discussion boards, virtual learning environments, etc.) responsibly. I will not use digital devices or the Internet to send or post hate or harassing mail, pornography, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors either at school or at home. I understand that I am to notify an adult immediately if by accident I encounter materials which violate appropriate use.
- I understand that I represent the school district in all my online activities. I understand that what I do on social networking websites should not reflect negatively on my fellow students, teachers, or on the District. I understand that I will be held responsible for how I represent myself, my school and/or the District on the Internet.
- I understand that masquerading, spoofing, or pretending to be someone else is forbidden. This includes, but is not limited to, sending out e-mail, creating accounts, or posting messages or other online content (e.g. text, images, audio or video) in someone else's name.
- I will use technology resources productively and responsibly for school-related purposes. I will avoid using any technology resource in such a way that would disrupt the activities of other users.
- I will refrain from attempting to bypass or circumvent security settings or Internet filters, or interfere with the operation of the network by installing illegal software, or web-based services and software not approved by the Stafford's District Technology Department.
- I understand that vandalism is prohibited. This includes but is not limited to modifying or destroying equipment, programs, files, or settings on any computer or other technology resource.
- I will respect the intellectual property of other users and information providers. I will obey copyright guidelines. I will not plagiarize or use other's work without proper citation and permission.
- I will only connect my own devices to the school's network in accordance with Policy 5131.84 Use of Private Technology Devices by Students.
- I will refrain from the use of or access of files, software, or other resources owned by others. I will use only those school network folders that are designated for my use or for the purpose designated by my teacher.

- I will follow all guidelines set forth by the District and/or my teachers when publishing schoolwork online (e.g. to a website, blog, wiki, discussion board, podcasting or video server).
- I understand the Internet is a source for information that is both true and false; and that the school is not responsible for inaccurate information obtained from the Internet. I agree to abide by all Internet safety guidelines that are provided by the school and to complete all assignments related to Internet safety.
- I understand that District administrators will deem what conduct is considered inappropriate use if such conduct is not specified in this agreement.

Please return this agreement, signed by the student and parent / guardian, to your child' s teacher or school office.

STUDENTS ARE REQUIRED TO SIGN AND RETURN THE APPLICATION FOR NETWORK ACCESS BEFORE THE USE OF ANY TECHNOLOGY EQUIPMENT (PERSONAL OR DISTRICT-OWNED) IS ALLOWED AT STAFFORD PUBLIC SCHOOLS.

Student's Full Name: _____

Home Address: _____

Home Phone. _____

School: _____

Home Room Number / Teacher: _____ Grade: _____

If you are a new student, please provide a password for network access (minimum of 6 numbers and letters)

Student Agreement / Consequences For Violation Of This Agreement

As a user of the School's technology resources, I understand and agree to comply with the specific terms and conditions for users as outlined in this Acceptable Use Agreement for Middle and High School Students. I also understand that I am responsible for any transactions that occur under my user ID or account whether it be on or off-campus and that any violation of the Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology may result in denied access to the district's technology resources, in addition to other disciplinary action.

Should I commit a violation, I understand that consequences of my actions could include suspension or loss of computer privileges or data and files, disciplinary action up to and including expulsion, and/or referral to law enforcement.

Student Signature: _____ Date: _____

Parent/Guardian Agreement

By signing below, I certify that all the information that I have provided on this form is correct and that I, as the Parent or Legal Guardian of the above named child, acknowledge and agree to the following:

- I have read and discussed this Acceptable Use Agreement with my child. I also understand that this agreement will be valid through October 1 of the following school year.
- I fully understand that this access is designed for educational purposes in keeping with the academic goals of the district, and that student use for any other purpose is inappropriate.
- I recognize that while every effort will be made to filter out controversial material, it is impossible for the Stafford School District to restrict access to all controversial material, and I will not hold Stafford Public Schools responsible for controversial material offered on the network.
- I understand that my child is responsible for any transactions that occur under his or her user ID or account whether it be on or off campus and that any violation of the Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology may result in my child being denied access to the district's technology resources, in addition to other disciplinary action.

I understand that my child will use the Stafford Public Schools Network and have Internet access. I also understand the school could be publishing examples of my child's projects or publish photographs/video of my child participating in school related activities in district media or share with local media outlets. Unless otherwise notified in writing by a parent or guardian, the school will assume permission is given to publish students' names, work, videos, and photographs.

Parent/Guardian's Name (print) _____

Parent/Guardian's Email _____

Parent/Guardian's Signature: _____

Date: _____

Students

Use of Private Technology Devices by Students

Students may possess privately owned technological devices on school property and/or during school-sponsored activities, in accordance with the mandates of this policy and any applicable administrative regulations as may be developed by the Superintendent of Schools.

Definitions

Board Technology Resources

For the purposes of this policy, "Board technology resources" refers to the Stafford Board of Education's (the "Board's) computers and instructional technologies; communications and data management systems; informational technologies and the Internet; and any other technology resources owned and/or used by the school district and accessible by students.

Privately Owned Technological Devices

For the purposes of this policy, "privately owned technological devices" refers to privately owned desktop computers, wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. These devices may include, but are not limited to, desktops, personal laptops, Smartphones, network access devices, Kindles, Nooks, cellular telephones, radios, personal audio players, I-Pads or other tablet computers, walkie-talkies, Blackberries, personal data assistants, I-Phones, Androids and other electronic signaling devices.

Use of Privately-Owned Technological Devices

The District provides an electronic device for every student and all students are expected to utilize the device provided while on school grounds in accordance with Board policy 6160.2 One-to-One Device Program. Privately-owned technological devices may not be used during instructional time, except as specifically permitted by instructional staff or administration, or unless necessary for a student to access the district's digital learning platform or otherwise engage in remote learning.

On school property, at a school sponsored activity, while in use for a remote learning activity, or while being used to access or utilize Board technology resources, the use of any such device for an improper purpose is prohibited. Improper purposes include, but are not limited to:

- Sending any form of a harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);
- Gaining or seeking to gain unauthorized access to Board technology resources;
- Damaging Board technology resources;

- Accessing or attempting to access any material that is obscene, obscene as to minors, or contains pornography;
- Cyberbullying;
- Using such device to violate any school rule, including the unauthorized recording (photographic, video, or audio) of another individual without the permission of the individual or a school staff member; or
- Taking any action prohibited by any Federal or State law.

Search of Privately Owned Technological Devices

A student's privately owned technological device may be searched if the device is on Board property or in a student's possession at a school-sponsored activity and if there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school. Any such search shall be reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.

Responsibility for Privately Owned Technological Devices

Students are responsible for the safety and use of their privately owned technological devices. If a privately owned technological device is stolen, lost, or damaged while the device is on school property or during a school sponsored activity, a report should be made to the building principal, who will investigate the loss in a manner consistent with procedures for stolen or damaged personal property. Students and parents should be aware that the Board is not liable for any privately owned technological device that is stolen, lost, or damaged while at school or during a school-sponsored activity. For that reason, students are advised not to share or loan their privately owned technological devices with other students.

Disciplinary Action

Misuse of the Board's technology resources and/or the use of privately-owned technological devices to access or utilize the Board's technology resources in an inappropriate manner or the use of such devices in any manner inconsistent with this policy will not be tolerated and will result in disciplinary action. For students, a violation of this policy may result in loss of access privileges, a prohibition on the use and/or possession of privately-owned technological devices on school property or at school-sponsored activities, and/or suspension or expulsion in accordance with the Board's policies related to student discipline.

Access to Board Technology Resources

The Board's may permit students, using their privately owned technological devices, to access the Board's computers and instructional technologies; communications and data management systems; informational technologies and the Internet; and any other technology resources used by the school district and accessible by students. Additionally, it is the expectation of the Board that students who access these resources while using privately owned technology devices will act at all times appropriately in ways which are fully in accord with applicable policies concerning technology use as well as all local, state, and federal laws.

Through the publication and dissemination of this policy statement and others related to use of the Board's computer systems, as well as other instructional means, the Board educates students about the Board's expectations for technology users.

The Board technology resources shall only be used to access educational information and to promote learning activities both at home and at school. Students are expected to act at all times appropriately in ways which are fully in accord with applicable policies concerning technology use as well as all local, state, and federal laws when using the Board technology resources. Failure to do so will result in the consequences outlined herein and in other applicable policies (including, but not limited to, the Safe School Climate Plan, the Student Discipline Policy and the Student Use of the District's Computer Systems and Internet Policy).

Students must abide by the procedures outlined in this policy and all policies and applicable regulations outlined in the Board's computer use and other applicable policies. Students will be given specific information for log-on and access procedures for using school accounts. No user may deviate from these log-on/access procedures. **Students are advised that the Board's network administrators have the capability to identify users and to monitor all privately owned technological devices while they are logged on to the network.** Students must understand that the Board has reserved the right to conduct monitoring of Board technology resources and can do so despite the assignment to individual users of passwords for system security. Any password systems implemented by the Board are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user. The system's security aspects, message delete function and personal passwords can be bypassed for monitoring purposes. Therefore, students should be aware that they should not have any expectation of personal privacy in the use of privately owned technological devices to access Board technology resources. This provision applies to any and all uses of the Board's technology resources and any privately owned technological devices that access the same.

Harm to Board Technology Resources

Any act by a student using a privately owned technological device that harms the Board technology resources or otherwise interferes with or compromises the integrity of Board technology resources will be considered vandalism and will be subject to discipline and/or appropriate criminal or civil action.

Closed Forum

This policy shall not be construed to establish a public forum or a limited open forum.

Legal References:

Conn. Gen. Stat. § 10-233j

Conn. Gen. Stat. § 31-48d

Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250, *et seq.*

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 28 U.S.C. §§ 2510 through 252

Policy adopted: June 25, 2012
Policy reviewed: August 20, 2012
Policy reviewed: January 30, 2017
Policy revised: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

Students

Use of Private Technology Devices by Students

The following guidelines shall govern the manner in which the Use of Private Technology Devices by Students policy and is to operate within the District.

Definitions

A "device" as part of this protocol is a privately owned and/or portable electronic handheld technology that includes emerging mobile communication systems and smart technologies, laptops and netbooks, and any technology that can be used for wireless internet access, word processing, image capture/recording, sound recording and information transmitting, receiving, and storing.

Teachers' Role

1. Teachers are facilitators of instruction in their classrooms. Therefore, they will not spend time on fixing technical difficulties with students' personal devices in the classrooms. They will educate and provide guidance on how to use a device and troubleshoot simple issues, but they will not provide technical support. This responsibility resides at home with parents/guardians.

2. Teachers may communicate information regarding educational applications and suggest appropriate tools that can be downloaded to personal devices at home. Parents will need to assist their younger children with downloads if they wish to follow teachers' suggestions.

3. Teachers will closely supervise students to ensure appropriate use of technology in the classrooms.

4. It is understood that the District provides each student with an electronic device and all students are expected to utilize the device provided while on school grounds in accordance with Board Policy 6160.2 One-to-One Device Program.

5. The use of these student personal devices in grades 9-12, as with any personally owned device, is strictly up to the teacher.

Security and Damages

1. The District, or any of its schools, is not liable for any device that is stolen or damaged. Responsibility to keep the device secure rests with the individual owner. If a device is stolen or damaged, it will be handled through the administrative office as other personal items are stolen or damaged. It is recommended that skins, decals, and other custom

touches be used to identify physically a student's device from others. Additionally, protective cases for technology are encouraged.

2. Personal devices cannot be left unsecured on campus before or after school hours.

Operating Principles for Use of Personal Devices on School Campus

1. Devices cannot be used during assessments, unless otherwise directed by a teacher. Students must immediately comply with teachers' requests to shut down devices or close the screen. Devices must be in silent mode and put away when asked by teachers.

2. Students are not permitted to transmit or post photographic images/videos of any person on campus on public and/or social networking sites.

3. Personal devices must be charged prior to bringing them to school and run off their own batteries while at school.

4. To ensure appropriate network filters, during school hours, students will only use the District provided electronic device while on school grounds in accordance with Board Policy 6160.2 One-to-One Device Program. and will not attempt to access the District network with a privately owned device, unless otherwise approved by administration.

5. Students must be instructed that bringing devices on campus or infecting the network with a virus or program designed to damage, alter, destroy, alter, or provide access to unauthorized data or information is in violation of the District's Acceptable Use Agreement and will result in disciplinary actions.

6. The District has the right to collect and examine any device that is suspected of causing problems or is the source of an attack or virus infection.

7. Students must be instructed that possessing or accessing information on school property related to "hacking", altering, or bypassing network security policies is in violation of the Acceptable Use Policy and will result in disciplinary actions.

8. Students can only access content on their device and/or Internet sites which are relevant to the classroom curriculum and/or authorized by a teacher.

9. Printing for academic purposes from personal devices may only occur if students are logged into their personal district Google account.

10. Personal devices may not be used to cheat on assignments, tests or for non-instructional purposes at unauthorized times, or in a manner in violation of our Acceptable Use Agreement and corresponding policy.

11. Personal devices may not be used to send inappropriate e-messages during the school day.

Standards of Responsible Use

All students in District schools must adhere to the following standards of responsible use:

- The District may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.
- Students are responsible at all times for their use of the District's electronic communication system and must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.
- Students must log in and use the District filtered wireless network during the school day on personal electronic devices.
- Students must not access, modify, download, or install computer programs, files, or information belonging to others.
- Students must not waste or abuse school resources through unauthorized system use (e.g. playing online games, downloading music, watching video broadcasts, participating in chat rooms, etc.).
- Students must not alter computers, networks, printers or other equipment except as directed by a staff member.
- Technology, including electronic communication, should be used for appropriate educational purposes only and should be consistent with the educational objectives of the District.
- Students must not release personal information on the Internet or electronic communications.
- If a student finds an inappropriate site or image, he or she must immediately minimize the program and contact the instructor.
- Students shall not use electronic devices in a manner which poses a threat to academic integrity, disrupts the learning environment, or violates the privacy of others. Students must not create/publish/submit or display any materials/media that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal and should report any instances encountered.
- Students shall adhere to all laws and statutes related to issues of copyright or plagiarism.
- Violation of any of these standards may result in suspension of computer use, Internet privileges and/or other disciplinary action.

Regulation approved: June 25, 2012
Regulation reviewed: August 20, 2012
Regulation reviewed: January 30, 2017
Regulation reviewed: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

Use of Private Technology Devices by Students - Instructional Time

The use of technology to provide educational material is a privilege at school that we wish all students. When abused, privileges will be taken away. When respected, they will benefit the learning environment tremendously.

Students and parents who bring their own device must adhere to the Student Code of Conduct as well as all Board policies, particularly the Internet Acceptable Use and Internet Safety.

At the discretion of the building administrator, personal devices may be used during noninstructional time such as but not limited to lunch period, hallway passing time, and before and after school hours provided they are connected to the school network.

Students acknowledge the following:

- During instructional time, only the school's Internet will be accessed. Attempts will not be made to bypass the local connection.
- The District's network filters will be applied to one's connection to the Internet and attempts will not be made to bypass them.
- Only authorized data can be accessed. Infecting the network with a virus, Trojan, or program designed to damage, alter, or destroy the network; and hacking, altering, or bypassing security policies are not allowed.
- The school District has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.
- All school-related data must be stored on the student's network drive or Google Drive. Such data from external storage devices must be transferred to the student's network drive or Google Drive.
- As we are working to achieve a more paperless environment, printing from a personal device is permissible provided that he/she is logged into his/her school district Google account.
- As we do not have enough outlets for students to charge their devices in classrooms, each student must charge his or her own device prior to bringing it to school daily.
- Using a personal device to transmit or share inappropriate content during the school day will result in the loss of privileges associated with this policy. Additional disciplinary consequences may be applied depending upon the circumstances. Transmission of material of a bullying nature or sexual nature will not be tolerated.
- The purpose of this policy is purely for the extension and enrichment of the learning environment. Each school shall develop and communicate a policy specific to the appropriate use of personal devices.
- Students must immediately comply with teachers' requests to shut down devices or close the screen. Devices must be in silent mode and put away when asked by teachers.

Use of Private Technology Device Agreement

- Students are not permitted to transmit or post photographic images/videos of any person on campus on public and/or social networking sites without prior written authorization from the building administrator.
- Students shall not use electronic devices in a manner which poses a threat to academic integrity, disrupts the learning environment, or violates the privacy of others. Students must not create/publish/submit or display any materials/media that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal and should report any instances encountered.
- Students can only access content on their device and/or Internet sites which are relevant to the classroom curriculum and/or authorized by a teacher.
- During school hours, devices are to be used for instructional purposes connected to the approved curriculum, not to cheat on assignments or tests, not to make personal phone calls, not to send text messages, and not to post information, photos, or videos not authorized by the teacher.
- Making personal phone calls can only occur during non-instructional time at the discretion of the building administrator. Sending text messages can only occur before/after school hours at the discretion of supervising staff.
- Personal devices may not be used to send inappropriate e-messages during the school day.
- Using a personal device at unauthorized times, or in a manner in violation of our Acceptable Use Agreement and corresponding policy, will result in the loss of privileges.

As a student, I understand and will abide by all guidelines in this agreement. I further understand that any violation is unethical and may result in the loss of my device privileges as well as other disciplinary action.

As a parent/guardian, I understand that my child will be responsible for abiding by the policy pertaining to this program and its guidelines. I have read and discussed them with him/her and he/she understands the responsibility he/she has in the use of their personal device.

Student Signature:	_____	Parent/Guardian Signature:	_____
Printed Name:	_____	Printed Name:	_____
Date:	_____	Date.	_____

After reading, please complete and sign the Use of Private Technology Device Agreement and return it to your child's school, as directed.

Instruction

One-to-One Device Program

The Board of Education (the "Board") recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. It is a goal of the Board to provide students and staff with access to a robust and comprehensive infrastructure when and where they need it for learning. The Board directs the Superintendent or designee to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

The Board believes the implementation of a one-to-one device program will provide the necessary tools and resources for a technology-rich learning environment characterized by flexibility, collaboration, personalization, and creativity. Learners will have engaging and empowering experiences in both formal and informal settings that prepare them to be active, creative, knowledgeable, and ethical participants in our globally connected society. Technology will enable students and staff to communicate, learn, share, collaborate, think and solve problems, manage their work, and take ownership of their lives. The program will allow student use of technology to mirror that of an adult who accesses technology-based tools when appropriate for a task.

Learning in District schools must be a continuous, dynamic interaction among students, parents, and the extended community. The one-to-one program enables anywhere, anytime learning that is not limited by the physical confines of a classroom or school building. The Board believes that purposeful technology integration assists teachers in shifting from being deliverers of content, and instead, allows them to be facilitators of deep, individualized learning for all students.

The policy, procedures, and information within this document apply to all District-owned devices used in District schools, including any other device considered by the administration to come under this policy. Individuals or teams of teachers may set additional requirements for use in their classroom.

Legal Reference: Connecticut General Statutes
10-221 Boards of Education to prescribe rules 18 U.S.C. §§ 2510-2522
Electronic Communication Privacy Act P.L. No 110-385
Protecting Children in the 21st Century Act

Policy adopted: August 23, 2021

STAFFORD PUBLIC SCHOOLS
Stafford Springs, Connecticut

Instruction

One-to-One Device Program

1. Device Check-in and Check-out

1.1 Device Check-Out

Devices will be checked out each fall to incoming students. Parents and students must sign and return the Device Protection Plan (DPP), Acceptable Use Agreement, and Device Loan Agreement before the device can be issued to a student.

1.2 Device Check-in

All devices, cases, chargers, and school-provided accessories must be returned at the end of each school year to be updated, serviced, and stored safely for the summer. Students, who graduate early, withdraw, are suspended or expelled, or terminate enrollment in the District for any other reason, must return their individual school device on the date of termination.

If a student fails to return the device at the end of the school year or upon termination of enrollment in the District, that student will be charged the replacement cost of the device, and may be subject to criminal prosecution or civil liability.

Just like a textbook or a band uniform, the devices are the property of the District, and students are responsible for returning them in reasonable condition. Any loss of or damage to a device is the responsibility of the student and will be handled in a manner consistent with the student's DPP. Students will be charged for repairs in accordance with the DPP, or the actual cost of any needed repairs should the DPP not be selected. Needed repairs will not exceed the replacement cost of the device.

2. Taking Care of Your Device

Students are responsible for the general care of the device they have been issued by the school. Devices that are broken or fail to work properly should be turned into the Library Media Specialist or building representative in the Library Media Center.

2.1 General Precautions

- The device is school property and all users will follow this policy and the District's acceptable use policy for technology.
- Only use a clean, soft cloth to clean the screen, no cleansers or liquids of any type.
- Cords and cables must be inserted carefully into the device to prevent damage.
- Devices and cases must remain free of any writing, drawing, stickers, or labels that are not the property of the District.

- A device should always be locked or supervised directly by the student to whom it is assigned. For instance, devices should never be left in an unlocked locker, unlocked car, or any unsupervised area.
- Students are responsible for keeping their device's battery charged for school each day.

2.2 Carrying Devices

The protective cases provided with devices have sufficient padding to protect the device from normal treatment and provide a suitable means for carrying the device within the school. The guidelines below should be followed:

- Devices should always be within the protective case provided by the District.
- No other items should be stored or carried within the device case to avoid pressure and weight on the screen.

2.3 Screen Care

The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the device when it is closed.
- Do not place anything near the device that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Clean the screen with a soft, dry cloth or anti-static cloth.
- Take care not to bump the device against lockers, walls, car doors, floors, etc., as it will eventually break the screen.

3. Using your Device at School

Devices are intended for use at school each day. In addition to teacher expectations for device use, school messages, announcements, calendars, and schedules may be accessed using the device. Students in Grades 6-12 must be responsible to bring their charged device to all classes, unless specifically instructed not to do so by their teacher. PreK-5 devices will be stored in charging stations in each classroom. Those students may be required to take devices home should a remote learning day be necessary.

3.1 Devices Left at Home

If students leave their device at home, they are responsible for getting the course work completed as if they had their device present. Students who repeatedly (as determined by any staff member) leave their device at home, will be required to leave their devices at school and check it out/in from a designated staff member at the beginning and end of each day.

3.2 Device Undergoing Repair

Loaner devices may be issued to students when they leave their devices for repair. There may be a delay in getting a device should the school not have enough to loan.

3.3 Charging your Device's Battery

Devices must be brought to school each day in a fully charged condition. Students need to charge their devices each evening, as a limited number of cords will be available in classrooms. Students who repeatedly (as determined by any staff member) fail to bring their devices to school charged will be required to leave their devices at school and check it out/in from a designated staff member at the beginning and end of each day.

3.4 Screensavers/Background Photos

- Inappropriate media may not be used as a screensaver or background photo.
- Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols or pictures will result in disciplinary actions.

3.5 Sound, Music, Games, or Programs

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Music (no videos) is allowed on the device and can be used at the discretion of the teacher.

3.6 Printing

Printing will be available with the device on a limited basis. Students should talk to their teachers about when and how to print.

3.7 Home Internet Access

Students are allowed to set up wireless networks on their devices. This will assist them with device use while at home. Students are not required to have wireless access at home.

4. Managing your Files & Saving your Work

4.1 Saving to the Device

Students may save work on their devices when working off line. Limited storage space will be available on the device for off line files – BUT it will NOT be backed up in case of re-imaging. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work. Teachers will instruct students on methods of managing workflow.

4.2 Network Connectivity

The District makes no guarantee that their network will be up and running 100% of the time. In the rare case that the network is down, the District will not be responsible for lost or missing data.

5. Software on Devices

5.1 Originally Installed Software

All software/Apps/games must be District provided and those originally installed by the District must remain on the device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular course. The licenses for this software require that the software be deleted from devices at the completion of the course. Periodic checks of devices will be made to ensure that students have not removed required apps.

5.2 Additional Software

Students are not allowed to load extra software/apps on their devices. The district will synchronize the devices so that they contain the necessary apps for school work.

5.3 Inspection

Students may be selected at random to provide their device for inspection. Devices are the property of the District and may be confiscated at any time. Each device will be collected and inspected at the end of each school year.

5.4 Procedure for Re-loading Software

If technical difficulties occur or illegal software, non-District installed apps are discovered, the device will be restored from backup. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

5.5 Software upgrades

Upgrade versions of licensed software/apps are available from time to time. Students may be required to check in their devices for periodic updates and synching.

6. Acceptable Use

The use of the District's technology resources is a privilege, not a right, and are in alignment with Board Policy and Regulation 5131.83 *Student Use of District's Computer Systems and Internet Safety*. The privilege of using the technology resources provided by the District is not transferable or extendible by students to people or groups outside the District and terminates when a student is no longer enrolled in the District.

These guidelines are provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy and its administrative regulations, privileges may be terminated, access to the school District technology resources may be denied, and disciplinary action may be sanctioned.

Violations may result in disciplinary action up to and including suspension/expulsion for students. When applicable, law enforcement agencies may be involved.

6.1 Parent/Guardian Responsibilities

- Talk to your children about values and the standards that your children should follow on the use of the Internet just as you do on the use of all media information sources such as television, telephones, movies, and radio.
- All students will be issued a device and students will be expected to utilize the District device to complete all school work. Personal devices should not be brought to school.

6.2 School Responsibilities are to:

- Provide Internet access and provide an individual Google account to its students.
- Provide Internet Blocking of inappropriate materials on District networks.
- Immediately report any inappropriate digital content to the building principal.
- Provide network data storage areas. These will be treated similar to school lockers.
- The District reserves the right to review, monitor, and restrict information stored on or transmitted via District owned equipment and to investigate inappropriate use of resources.
- Provide guidance to aid students in use of the device and help assure student compliance of the acceptable use policy.

6.3 Students are Responsible For:

- Using computers/devices in a responsible and ethical manner.
- Obeying general school rules concerning behavior and communication that apply to device use.
- Using all technology resources in an appropriate manner so as to not damage school equipment. This "damage" includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by the students own negligence, errors or omissions. Use of any information obtained via the District's designated Internet System is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- Helping the District protect our computer system/device by contacting any staff member about any security problems they may encounter.
- Monitoring all activity on their account(s)/device.
- Securing their device after they are done working to protect their work information and device.

- Notifying an adult immediately should they receive inappropriate digital content.
- Returning their device at the end of each school year. Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment for any other reason, must return their individual school device computer on the date of termination.

6.4 Student Activities Strictly Prohibited:

- Illegal installation or transmission of copyrighted materials.
- Any action that violates existing Board policy or public law.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Use of outside data disks or external attachments without prior approval from the administration.
- Changing of device settings (exceptions include personal settings such as font size, brightness, etc.).
- Downloading apps.
- Spamming-sending mass or inappropriate emails.
- Gaining access to other student's accounts, files, and/or data.
- Use of the school's Internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Use of anonymous and/or false communications.
- Students are not allowed to provide personal information over the Internet – with the exception of teacher-directed instances.
- Participation in any form of illegal behavior.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass, demean, or bully recipients.
- Bypassing the District's web filter through a web proxy.

6.5 Device Care

Just like any school property issued to a student for individual use, students will be held responsible for maintaining their individual devices and keeping them in good working order. Students are responsible for any and all damage. A Device Protection Plan (DPP) is available through the District.

- Devices that malfunction or are damaged must be reported immediately. All device repairs must be handled through the District. Students are responsible for the actual cost of damages – not to exceed the cost of replacement.
- Device batteries must be charged and ready for school each day.
- Device cases furnished by the school District must be returned with only normal wear and no alterations to avoid paying a case replacement fee.
- Devices that are stolen must be reported immediately to a building administrator.

6.6 Legal Propriety

- Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. Questions may be posed to any school official.
- Plagiarism is a violation of the District's Code of Conduct. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- Use or possession of hacking software is strictly prohibited and violators will be subject to discipline. Violation of applicable state or federal law will result in criminal prosecution or disciplinary action by the District.

7. Protecting and Storing your Device

7.1 Device Identification

Student devices will be labeled in the manner specified by the school. Devices can be identified in the following ways:

- Record of serial number
- District label

7.2 Storing your Device

When students are not using their devices, they should be stored in a secure environment, such as a locked locker. Nothing should be placed on top of the device at any time as pressure may cause the screen to crack. Students in Grades 6-12 should take their devices home each day, regardless of whether or not they are needed. Devices should not be stored in a vehicle at school or at home. Devices for students in Grades PreK-5 will store their devices in charging stations located in their classroom.

7.3 Devices Left in Unsupervised Areas

Under no circumstances should devices be left in unsupervised area. Unsupervised areas include the school grounds and campus, the lunchroom, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, and hallways. Any device left in these areas is in danger of being stolen. If a device is found in an unsupervised area, it will be taken to the office and dealt with as a disciplinary matter.

8. Repairing or Replacing your Device

8.1 School District Protection

The District provides a Device Protection Plan (DPP) for students and parents to cover device replacement. The DPP coverage for the school year costs $35 per device. No family will be charged more than $105 (cost of coverage for three (3)

students). Those families requiring financial assistance may contact their child's school office. Policies purchased mid-year will not be prorated and will follow the same pricing structure. The plan includes the first repair of any part of the device, up to three separate repairs, as long as the damage is not due to the negligence of the user or malicious behavior. Devices in need of repair that were not kept in the protective case provided by the District will be charged a $20 copay for each instance of repair.

8.2 Multiple Claims

Multiple damage/theft claims, especially if lack of due diligence is evident, could result in assessment of full repair cost, replacement cost, or restriction of take-home privileges.

8.3 Loaner Devices

Loaner devices cannot be issued until financial obligations have been arranged for or payment has been made to school officials.

9. Cost of Repairs

Students will be held responsible for ALL damage to their devices including, but not limited to: broken screens, cracked plastic pieces, inoperability, etc. Should the cost to repair exceed the cost of purchasing a new device, the student will pay for full replacement value. Lost items such as cases and cables will be charged per the DPP, should the plan be chosen, or actual replacement cost.

6160.2 (a) REG
Form

Stafford Public Schools
Student Device Loan Agreement

Responsibilities

By signing the *Stafford Public Schools Acceptable Use Agreement and Application for Network Access*, parents / guardians and students have agreed to follow the guidelines contained within it, and all local, state, and federal laws. Any violation of any of these policies may result in a loss of network privileges, loss of right to use the device, and / or discipline.

The use of district issued technology is a privilege and intended for school purposes only. By accepting a district issued device the following conditions shall apply:

- Suspicious links will be avoided, and the manufacturer's operating system will not be replaced with custom software (i.e. "jailbreaking" the device).
- All accounts and/or passwords will be kept secure and will not be shared with other individuals. This includes passwords for email and / or network access.
- Email and other computer communication media should only be used for appropriate, legitimate, and responsible communication.
- Stafford Public Schools is not responsible for loss of data. It is the user's responsibility to store and backup files.
- Only district staff are authorized to repair a district issued device.
- Stafford Public Schools personnel have remote access to the device and/or files, and are allowed to utilize this access at any time should an issue arise.

Proper Care

Proper care of the district issued device is required. Guidelines for proper care are listed below.

- The device should be kept in a secure location at all times.
- The device should never be dropped.
- The device should never be left in places of extreme hot or cold temperatures, humidity, or limited ventilation for an extended period of time.
- The device should only be cleaned with a soft cloth.
- Eating or drinking when using the device should be avoided.
- Defacing the device in any manner is prohibited (including the addition of stickers and labels).

6160.2 (b) REG
Form

Acknowledgement

Parents / Guardians / Students

Parents / guardians agree to review with their child the *Stafford Public Schools Policies, Regulations and Forms Governing the Use of Technology*, as were provided at the beginning of the school year (copy available at www.stafford.k12.ct.us, under "For Parents") and ensure that their child follows the principles of good digital citizenship.

By signing this Agreement below, parents / guardians acknowledge the following:

- ✓ I have read, understand, and agree to the terms and conditions outlined in this Agreement.
- ✓ I understand that the condition of this device will be documented upon distribution. I further understand that I am financially responsible for loss or damage due to neglect and will be required to reimburse the district, up to full replacement cost.
- ✓ I agree to return the district issued device and any accessories provided by the district, when requested to do so or at the time of withdrawal from the Stafford Public Schools, whichever comes first.

Signature of Parent / Guardian: _____ Date: _____

Printed Name: _____

Signature of Student: _____ Grade: _____

Printed Name: _____ Date: _____

Parents / Guardians should return this form to your child's school.

Stafford Public Schools

Device Protection Plan (DPP)

2021 – 2022 School Year

Please Note:

The protection plan is purchased EACH school year. Previous school year payment does not cover current school year.

Revised July 27, 2021

INTRODUCTION

Care of all instructional materials, including Chromebooks and iPads, distributed by STAFFORD PUBLIC SCHOOLS is the responsibility of the student to which they are assigned and his/her parent or legal guardian. This includes costs associated with damages, loss or theft. The purpose of the Device Protection Plan (referred to as DPP) is to protect STAFFORD PUBLIC SCHOOLS families from accumulating debt due to accidental damage or theft (see definitions below) of school-issued devices. A separate form must be completed for each device covered; one form per student. If you do not elect this program, the device replacement and/or damage costs are fully paid by the family.

PLAN TERM

- Policies run per school year, starting the 1st of August 2021 to the end of July 2022.
- Students issued devices at the beginning of the regular school year may purchase the DPP until the last day of August 2021.
- New students starting after the first day of school may purchase the DPP at the time of registration. DPP information needs to be turned in within three (3) weeks of registration.
- Policies purchased will terminate the last day of July of that school year.

COST

DPP coverage for the 2021-2022 school year costs $35 per device. Those families requiring financial assistance may contact Diane Peters, Business Manager. Families with more than three (3) children will be charged $105 (cost of three (3) children) to cover the cost of all children. Policies purchased mid-year will not be prorated and will follow above plan.

REFUNDS

Refunds are not available. Student transfers are covered under Plan Portability below.

REPAIRS

STAFFORD PUBLIC SCHOOLS will pay for the repair cost of the covered device to include parts and labor. If the device cannot be repaired, an equivalent replacement of STAFFORD PUBLIC SCHOOLS' choosing will be provided. If a replacement device is provided, this coverage will transfer to the replacement device for the duration of the current school year. While a student's device is being repaired the student will be issued a loaner device of STAFFORD PUBLIC SCHOOLS' choosing. This policy will cover the loaner device until the student's original device is returned or a permanent replacement device is issued.

PLAN SPECIFICATIONS (PER PLAN YEAR)

The first repair of any part of the device, up to three (3) different repairs, will be covered under the DPP as long as damage is not due to negligence or malicious behavior. An example of three covered parts would be: one screen, one keyboard, and one charger. For example, if multiple repairs to the same part are necessary (i.e. two (2) screens), the first screen would be covered under the DPP and the second and subsequent screens will incur charges based on the repair costs below. However, if repairs are required to one screen and one keyboard, the repairs would be covered by the DPP at no additional charge.

Devices in need of repair and covered under the elected DPP, however NOT kept in the protective case provided will be charged a $20 copay each instance of repair. Damage that occurs from lack of appropriate care of the device, or if the device is removed from the case, may not be deemed intentional and not accidental, therefore not being covered by DPP. This plan does not cover intentional damage by the covered student or household members. Assessment of any damage is determined by the Stafford Public Schools Instructional Technology Department.

	Chromebook	**iPad**
Sticker Removal *	$10	$10
Power Adapter	$50	$55
Screen replacement	$75	$100
Keyboard replacement without trackpad **	$35	N/A
Keyboard replacement with trackpad (missing keys or integrated trackpad)	$65	N/A
Trackpad only	$40	N/A
Top Cover	$40	N/A
Bottom Cover	$40	N/A
Charge for devices sent to Apple in addition to repair cost.	N/A	$49
Full device replacement	$265	$299
Case	$40	$40

* *Does not cover additional damage caused to device*.

****** *If part is available.*

******* *Other charges may be required due to damage and will be assessed at fair market value at time of repair.*

MISREPRESENTATION

Coverage may be revoked if the student willfully defrauds, conceals, and/or misrepresents any material information about the cause of damage or loss of the device.

Plan Includes:

- Accidental damage
- Theft or robbery (requires official police report)
- Vandalism (requires official police report or school administrator incident report)
- Fire, flood, natural disaster
- Power surge
- Device manufacturer defect

Plan Exclusions:

- Avoidable damage due to negligence
- Corrosion and rust
- Cosmetic damage (i.e. gouges to external casing, cracked or dented casings)
- Dishonest and/or intentional acts
- Unexplained loss or mysterious disappearance
- Government seizure
- Loss or damage to accessories, software and data
- Tampering with or attempts to repair device.

Plan Portability

If a student transfers to another STAFFORD PUBLIC SCHOOLS site during the plan term the coverage will transfer to the new site and remain in effect until the end of the term. If a student transfers to a site outside of STAFFORD PUBLIC SCHOOLS, the coverage does not transfer to the new district /school and the device must be returned to STAFFORD PUBLIC SCHOOLS, however, if the student returns to Stafford Public Schools at a later date in the same school year, the plan will still be in effect until the end of the original plan term. If a student leaves in the middle of a school year, coverage will not be refunded at a prorated amount.

Procedure for Lost or Damaged Devices

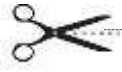
Report the loss or damage to the school administration and /or IT staff within 30 days. In the event that school is not in session, you must notify the Technology department by email.

SCHOOL	ADMINISTRATION	IT STAFF
SHS	Marco Pellicia: pelliccim@stafford.k12.ct.us Tim Kinel: kinelt@stafford.k12.ct.us	Email: help@stafford.k12.ct.us For more urgent matters call: 860-684-2218
SMS	Sue Mike: mikes@stafford.k12.ct.us Jon Campbell: campbellj@stafford.k12.ct.us	
SES	Mary Claire Manning: manningm@stafford.k12.ct.us Sara Varga: vargas@stafford.k12.ct.us	
WSS	Anna Gagnon: gagnona@stafford.k12.ct.us	

DEVICE PLAN PAYMENT

Payment can be made by cash or check. Checks should be made out to “Stafford Public Schools”. Please complete the below form and send in with payment to:

Stafford Public Schools
ATTN: Emily Wallach
16 Levinthal Run
Stafford Springs, CT 06076



PROTECTION PLAN REQUEST FORM

YES	NO
Iwould liketo participate in the DPP. I agree to the terms of participation including my responsibility for Damage or Loss not covered by theprogram. Payment (cash or check) is attached.	I decline to participate in the DPP. I understand that I am responsible for 100% of any Damage or Loss to the district issued device. Total replacement cost for the Chromebook is $265 device only or $300 including case. Total replacement cost for the iPad is $299 device only or $340 including case.
Date:	Date:
Parent Signature:	Parent Signature:
Print Name:	Print Name:
Student Name:	Student Name:
Grade:	Grade: