Shonto Governing Board of Education, Inc.
Policy Statement

SUBJECT: *TECHNOLOGY USE POLICY*
POLICY CODE: *GDU*
DATE OF ORIGINAL POLICY: 11/08/2005

EFFECTIVE DATE: January 8, 2021
DATE OF NEXT REVIEW:
DATED: 1/8/2021

I. INTRODUCTION:

The goal in providing these resources is to promote educational excellence in the District by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The Internet is a worldwide network of computers that has millions of pages of information. Users are cautioned that many of these pages include offensive and inappropriate materials. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an email address on the Internet may lead to receipt of unsolicited e-mail containing offensive content.

Users accessing the Internet do so at their own risk and Shonto Governing Board of Education, Inc. is not responsible for material viewed or downloaded by users from the Internet. The Children's internet Protection Act requires that the use of the resources be in accordance with its guidelines and support the education, research, and educational goals of the District Therefore, the Shonto Governing Board of Education, Inc., establishes the following policy.

I. POLICY STATEMENT:

This policy provides the procedures, rules, guidelines and codes of conduct for the use of the technology resources to its stakeholders at Shonto Preparatory Schools. The reduction of computer abuse provides adequate resources for users with legitimate needs. Through technology, the District provides access for students and staff to resources from around the world. Expanding technologies take students and staff beyond the confines of the classroom, and provide tremendous opportunities for enhancing, extending, and rethinking the learning process.

II. EXCEPTIONS TO POLICY:

Exceptions to district rules will be made for district designated agent(s) conducting an investigation of a use which potentially violates the law, district policy, regulations or rules. Exceptions will also be made for technology administrators who need access to district technology resources to support the district's resources or review the delete data stored on district computers.

Incidental and occasional personal use of district resources may occur when such use does not generate a direct cost for the District or interfere with an individual's work. Any such incidental and occasional use of District resources for personal purposes is subject to the provisions of this policy. Employees and students are reminded that such incidental use must comply with this

policy and all applicable policies, procedure and rules. The Shonto Governing Board of Education, Inc. reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

III. DEFINITION

Technology	The purposeful application of information in the design, production, and utilization of goods and services, and in the organization of human activities.
Internet	A means of connecting a computer to any other computer anywhere in the world via dedicated routers and servers.
Virus	A computer virus is a type of destructive code or program designed to change the way a computer functions and is created to spread from one computer to another.
Web content filter	A program or utility which seeks to detect advertising and other bothersome or undesirable content before its loaded onto a Web page being accessed.
Cyberbullying	Is the use of technology to harass, threaten, embarrass, or target another person.

IV. AMPLIFYING INSTRUCTIONS AND GUIDELINES:

A. ACCEPTABLE USE

Using the District technology for educational purposes and research consistent with the District's educational mission, curriculum, and instructional goals. The same rules and expectations that govern students and employee's conduct and communications will apply to the use of District technology. Users are further expected to comply with these rules and all specific instructions from the teacher, school principals, department supervisor, and/or school's administrators.

B. INTERNET USE

The Internet is an electronic network connecting millions of computers and individual users worldwide. The purpose of the Internet is to support world-wide access to a broad variety of information and data, and to allow the sharing of content created by a multitude of users. The use of an assigned District account must be in the application and support of educational and instructional technology, and must be consistent with the educational objectives of District and

the standards that have been established by Shonto Governing Board of Education, Inc. and its administration.

It is permissible to get access the District wireless Internet network where available using any personal computing device. However, access of the wireless Internet by a user means that the user agrees to all the rules and guidelines (Waiver of Rights) set in this document including adherence to the limitations of the Children's Internet Protection Access (CIPA) Content Filter. Additionally, users must not deliberately perform acts that waste technology resources or unfairly monopolize resources.

1. Internet access provided to employees for ***research, reporting and educational activities*** relating to their duties (and not for entertainment purposes). Employees may also use the Internet access for access to electronic mail, World Wide Web, Various discussion groups and social networks (which may be restricted by CIPA filtering), LIMITED Streaming Audio and Video content, web-based educational applications, SPS websites (web pages, blogs, training, etc.). ***Users are encouraged to remember that the District has limited Internet access.***
2. Network Etiquette – You are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:
    - Be polite. Do not be abusive in your messages to others.
    - Use appropriate language. Do not swear, use vulgarities or any other inappropriate or suggestive language. Illegal activities are strictly forbidden.
    - Do not reveal your personal address or phone number or that of other employees or students, except in your normal course of duties.
    - Note that SPS-provided e-mail accounts are not guaranteed to be private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
    - Use proper grammar/language when communicating "official" school business via email, text, i.e. Avoid using SMS Language, SMSish, text language, i.e.

C. SCHOOL ISSUED DEVICES

Periodically, there is a temporary short-term or long-term need to loan school equipment to users of Shonto Preparatory School. The policy permits such usage when appropriate procedures have been followed, and the request has been approved by a school administrator with the following additional conditions:

1. The borrower agrees to accept the responsibility for repairing or replacing the devices when the device is damaged beyond the normal wear and tear or lost.
2. The device is in good condition.
3. Must be returned immediately to the school when asked, and in good working condition.
4. Borrower agrees to take all Digital Citizenship courses as assigned within the specified time frame of 30 days upon receiving a device.

a. Students in Grades Kindergarten to Fifth will take Digital Citizenship courses in Google Classroom.
b. Students in Grades Sixth to Twelfth will take Digital Citizenship courses in Microsoft Team Meet (or Google Classroom).
c. Employees will take the Digital Citizenship courses in Applied Digital Skills Google, provide a certificate of completion for all assigned modules.

5. Borrowers shall have no expectations of privacy with respect to the content on the device(s). This includes, but not limited to, internet usage, phone calls, text messages, photos, email, chat, notes and applications.
6. Device(s) and related content are subject to provisions of the inspection of Public Records Act, including any personal information that may be housed on the district device(s). Pursuant to state statute, public records may not be intentionally destroyed once the information has been formally requested through the Custodian of Public Records. The provisions may be extended to their personal devices if their personal devices was used to engage in Shonto Governing Board of Education, Inc. related affairs such as using the WI-FI connection, using email account issued by the District, i.e.
    a. Users may request to use the District WI-FI network to complete District related tasks or activities. District Information Technology Department may revoke this privilege at any time if they deem it necessary, especially when the District's network may be at risk for viruses.
7. All school issued devices are connected to the District WI-FI network. The WI-FI credentials will be added to the devices, though the credential information will not be shared. Under no circumstances will the WI-FI passwords be shared outside of the District Informational Technology Department.

D. COMPUTER USE

Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the users or any other employee's job performance; b) have an undue effect on the computer or school network's performance; or c) violate any other policies, provisions, guidelines or standards of this agreement or any other of the school, state and federal laws. Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

Inappropriate use of any District computer or the District network can be a severe offense. Please note that it is a violation of District policy to:

1. Duplicate copyrighted software provided by the District. It is a criminal offense to copy ANY software that is protected by copyright, unless such copying is expressly provided for within the copyright agreement, and the District will treat it as such.
2. Use District licensed software in a manner inconsistent with the licensing agreement. Information on licenses is available from the Informational Technology Department.

3. Copy, rename, alter, examine, install or delete the files or programs of another person or District except in the case of an Information Technology personnel or a designated personnel who are troubleshooting or otherwise repairing a computer.
4. Using a District's computer or network to annoy others including, but not limited to, sending offensive/ mass messages or intentionally causing a computer system or network to crash.
5. Using a computer for non-school-related activities including, but not limited to, personal or private business (with the limited exception of using personal email during breaks such as lunch or non-working times). Except in extraordinary situations, all work-related email should be transmitted using District issued email accounts. Any use of personal email during working hours must meet the same standards as established throughout this document.
6. Create, disseminate, or run a self-replication program (virus, worm, or any program that inhibits operation of any computer or network whether it is destructive or not) or distributing large quantities of information that overwhelm any network including but not limited to chain letters, network games, inappropriate use of the "All Users" email address, mass copying of files, and so on.
7. Fail to consult with the Information Technology Department before making any technology purchases, downloads, updates or installations. It is a violation to purchase, download, install or use software, hardware, applications and/or peripherals on district equipment and networks that have not been expressly approved by the Information Technology Department. All purchases and downloads (including those with an official District purchase order) must be reviewed and approved by IT. Further, prior to purchase, users are responsible for forwarding the appropriate technical information to IT for their review and assessment. For all technology-related purchases, a copy of the license agreement must be forwarded to IT and the building administrator for tracking and audit purposes.
8. Download, install or run executable applications and software from the Internet, including the use of VPN/proxy servers to bypass the District "Content Filter" to run. Use of any VPN/proxy server to bypass the District Content Filter (as required by the Children's Internet Protection Act, CIPA - 2011) is considered a severe violation. Only IT may authorize the installation of technology purchases and, in most cases, only IT personnel are permitted to install such technology purchases.
9. Install personally purchased computers, hardware, software or peripherals (such as printers and scanners) on District computers or the District network with the limited exception of the wireless network described below. The IT may approve installation of personally-purchased software if requested by a building administrator and Information Technology department determines it to be compatible with District systems. If permission is attained, then a copy of the license agreement and the installation media must be housed with the administrator of that building for audit purposes.
10. Access the District network and programs with personal computers unless such programs

are made available by IT (such as the web-based email server or the web-based version). Personal computers may not be tied into the District network, either through wireless, VPN or LAN connections EXCEPT with the express permission of the Superintendent and/or the IT, and with security devices installed by IT. Further, the use of that computer will be subject to the policies and procedures outlined in this document.

11. Use portable storage devices, files and applications that might otherwise be blocked by the CIPA Content Filter. The use of portable storage devices (such as CD-RW, DVD-RW, USB flash drives, USB cords, iPad and iPods) and other devices (such as an Apple, Android, i.e.) on district equipment is permissible provided that such devices are used in a professional manner and do not violate any rules, policies or guidelines delineated in this document (including copyright laws).
12. Take, scan or publish pictures of individuals on school property without individual's permission or if it's a minor the permission of the parents/guardian on file and the permission from the building administrator. Additionally, no pictures of District property may be taken without an administrator's approval.
13. Post any political, commercial, pornographic or otherwise questionable material to the District web site or any District hosted web site. Additionally, any postings must meet general District Policies and be approved by the Information Technology Department, the Superintendent or an approved delegate.
14. Use personal email use for "official" school business (Outlook, Yahoo, Gmail, i.e.) unless prior approval is given by the Superintendent and department supervisor for employees and by building principal for students.
15. Access or attempt to access a desktop, network, or host computer without having obtained the appropriate access log-in ID and password legitimately. Further, it is considered a severe violation to share log-in and password information with another user; likewise, it is also a severe violation to use the log-in and password information of another user. These actions are considered "hacking" and/or "trespass" and will be dealt with appropriately.
16. Share, distribute or otherwise provide personal log-ins and password information with another individual other than representatives from the Information Technology Department. Individuals sharing passwords with others, especially students, will be subject to disciplinary action. All users are required to contact the Informational Technology Department immediately if they suspect that their password has been compromised. See Password Section for Guidelines.
17. Tamper with switch settings, hardware (including keyboards, monitors and mouse devices), or move, reconfigure, and/or do anything that could damage District property (including but not limited to hardware such as terminals, computers, printers, and other peripherals). Any individual responsible for causing damage in any manner to any District property (including but not limited to hardware, software, computer systems, or computer labs) will be FINANCIALLY responsible for all repairs and/or replacements. This includes, but is not limited to unplugging cables, plugging cables into inappropriate

locations, or other related activities that may cause the network or connection to the network to fail or to function improperly. The Business Office will confirm financial clearance otherwise official transcripts, record transfers, recommendations, i.e. will be withheld until all debts have been cleared.

18. Use District equipment, networks, software and systems without the proper training in the correct usage. All employees are required to receive the appropriate training in the use of District systems, software and equipment from their appropriate supervisor (or the supervisor's delegate); if an employee has not received training or is still uncertain as to their comfort level, they should contact the Technology Department or Curriculum, Assessment, Professional Development.
19. Users are required to properly shut down and restart their computers at least one time during the week to assure data is saved properly and general system upgrades can run accordingly.
20. Use the District network to store, record, download or otherwise procure and transfer music (such as streaming audio or Internet radio) or images (such as pictures and streaming video) for personal entertainment. Streaming audio and video is permissible for educational and training purposes. User's files may be purged of excessive audio and video data at any time at the discretion of the Superintendent, school principals or the Information Technology Department. It is permissible to request installation if iTunes and to play music from a portable device should be as an iPod, MP3 player, or mobile phone provided that the files are not transferred to the District network or any District computer.

V. PROHIBITED ACTIVITIES

Without prior written permission from school, the school's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, malware, adware, spyware, phishing, etc.) or any other unauthorized materials.

A. Inappropriate use of an account

The use of the Internet is a privilege, not a right. Inappropriate use will result in cancellation of privileges.

B. Cyberbullying

Cyber Bullying is the use of electronic information and communication devices to willfully and repeatedly harm either a person or persons through the medium of electronic text, photos, or videos.

Cyber Bullying and Harassment will not be tolerated. Students and employees, on a yearly basis, will take the assigned Digital Citizenship courses and complete within 30 days of receiving a device, or the start of the new fiscal or school year. Actions deliberately

threatening, harassing, intimidating an individual or group of individuals, placing an individual in reasonable fear of harm or damaging the individual's property; or disrupting the orderly operation of the school, will not be tolerated.

C. Communication of trade secrets.

Unless expressly authorized to do so, users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to school. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal Economic Espionage laws.

D. Virus Detection.

Files obtained from sources they are not expecting, including external hard drives, USB flash drives, USB Type C, SD Card, Nano SIM Card, cloud-base (Google Drive, One Drive, Dropbox, i.e.) brought from home, files downloaded from the internet, other online services; e-mail attachments, and/or files provided by customers or vendors, may contain dangerous computer viruses. Those viruses can damage the school's computer network. Users should never open e-mail attachment they are not expecting. The District provides anti-virus protection on all District computing devices. Information Technology Department will receives notification of infection, and depending on the severity of the issue you will be informed to bring the device back to school for an investigation.

If you suspect that a virus has been introduced into the school's network, notify the Information Technology Department immediately.

E. Blocking Sites with Inappropriate Content**.**

The school has the right to utilize software that makes it possible to identify and block access to internet sites containing inappropriate materials, seeking information to cause harm, cyberbullying, etc. using District resources, including the school WI-FI network.

VI. OWNERSHIP

All hardware, software, documents and data on retrievable medium residing on the District network or saved to file management systems including, but not limited to, network drives, USB flash drives, USB Type C, SD Card, Nano SIM Card, cloud-base (Google Drive, One Drive, Dropbox, i.e.) that are resident on District equipment, are and shall remain the property of Shonto Preparatory School. District administration reserves the right to confiscate, remove, search or otherwise investigate any of the above mentioned items at its discretion.

VII. PASSWORD

Passwords are an essential component of a network protection, specifically a user's identity and

information. It authenticates the user not only to a device but to the user's data. Passwords must be used and secured to ensure a degree of protection is met. The purpose is to provide guidance for District users to generate acceptable passwords to use and protect them in an appropriate manner.

Note: this list is not meant to be all-inclusive; it is given simply for reference purposes.

A. Password Construction Guidelines

1. Password should not be well-known, contain personal information, your name or username.
2. A minimum of eight (8) characters in length must use to access devices (Standard Workstations/Laptops and District Labs). Passwords must contain at least a one (1) lower case letter, one (1) upper case letter, one (1) number, and one (1) special character.
3. Passwords for accessing sensitive data (servers, routers, Firewalls, Switches) must be at least ten (10) characters long which must have a one (1) lower case letter, one (1) upper case letter, one (1) number, and one (1) special character

B. Password Protection

1. Passwords should be viewed as confidential. Under no circumstances will District user give another person their password, unless approved by the Superintendent, principal and/or Information Technology Department.
2. District users are encourage not to maintain an unsecured written record or an electronic file, of his or her passwords. If it is important to maintain a password record, it must be stored in a protected access managed form if it is in hard copy form or in an encrypted form if it is in electronic form.
3. District users are encouraged not use the application's "Know Password" function.
4. If an employee either discovers or believes that his / her password has been compromised, notify the Information Technology Department immediately.

VIII. CONSEQUENCES FOR INAPPROPRIATE USE

The Technology Department will deem what is inappropriate use and, after consulting with the Superintendent or appropriate supervisor, may close an account. Administrators may request the IT Department to deny, revoke, or suspend specific user's-accounts. If a user has failed to comply with this policy, he/she may be:

A. Removed from the system for a specific period of time or permanently, depending on the nature of the offense.

B. Required to pay for damages, technician time, computer resources, or other fees.

C. Criminally charged under local, state, or federal laws.

D. Subject to employee disciplinary action, up to and including termination or discharge in accordance with existing Board policies and applicable law.

IX. DELEGATION OF AUTHORITY

All supervisors or administrators are expected to review the contents of this policy annually with students and/or staff.

X. REPORTS

Employees and students suspected of inappropriate use will be subject to disciplinary action as outlined in the personnel manual or school handbook.

XI. FORMS

A. Loan Authorization of Technology Equipment (Employee)

B. Loan Authorization of Additional Technology Equipment/Accessories (Employee)

C. Laptop Loan Agreement Form (Student)

D. Replacement Device Review (Student)

E. Returning Device Review (Student)

F. Loan Agreement of Additional Technology Equipment/Accessories (Student)

XII. EXPIRATION DATE

This policy will be reviewed and revised as needed as technology is fluid and subject to change at a moment notice.

XIII. SIGNATURE BLOCK

Submitted by: Melvin Kowakuka Date: 01/08/2021

1st Reading: October 5, 2020

2nd Reading: December 30, 2020

3rd Reading: January 8, 2021

Established: Tom Franklin
Mr. Tom Franklin Jr., Board President
Shonto Governing Board of Education, Inc.