St. Thomas Aquinas Regional School
Technology Acceptable Use Policy

Purpose

Saint Thomas Aquinas Regional School (STARS) genuinely believes that technology plays a vital role in 21st century education. Therefore, STARS supports technology use in the classroom and is prepared to face the persistent challenges to the delivery, management, and support of effective teaching learning experiences.

To assure that technology will play an active yet balanced role in the educational process, STARS provides students, teachers, and staff with access to the internet and other technology resources as a means of increasing learning and productivity for the purpose of laying a strong foundation in preparation for high school and college.

For the purpose of this policy, technology is defined as, but not limited to, procedures the diocese and school impose on their use of technology such as Internet, social media, and electronic media resources, teacher and staff use of personal devices, and release of teacher and staff information.

In addition, this policy requires that users agree to abide by the Dioceses of Arlington's Education policies, the STARS computer guidelines, and stipulations of the Children's Online Protection Act 47 USC Section 231 (COPPA), the Family Education Rights and Privacy Act (FERPA), and the Children's Internet Protection Act (CIPA) as well as laws pertaining to stalking and harassment. The policy is promulgated so as to be in compliance with the public records laws of the State of Virginia.

The Policy

STARS establishes and maintains rules for appropriate technology utilization in STARS classrooms, administration, and management. STARS is committed to protecting the information that is critical to teaching and the school's varied activities, business operations, and the communities we support, including students, faculty, and staff. These protections may be governed by legal, contractual, or school policy considerations.

Everyone at STARS has a responsibility for proper handling and protection of confidential information as set out in the Policy Statements. These policies apply to staff, teachers, and students.

STARS has taken measures designed to protect students, teachers, and staff from offensive information and has restricted access to online materials that are unsafe for minors. Failure to follow all or part of this policy, or any action that may expose STARS to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or that may compromise the safety of users is prohibited and may result in disciplinary action up to and including loss of network privileges, confiscation of computer equipment, suspension, termination of employment, and/or criminal prosecution.

1.- **Faculty and Staff**

i. *Faculty and Staff Compliance*

Faculty and Staff are provided access to STARS' technology environment for academic use. All staff and teachers must comply with the STARS policy and assume responsibility for acting to preserve the integrity of these systems and any school data to which they may have access.

STARS personnel with issued devices must comply with the STARS policy. It is the responsibility of the teacher/staff member to perform and remain current with all necessary updates to include software and credentials on STARS owned devices.

ii. Faculty and Staff BYOT (Bring your Own Technology)

Faculty and staff may bring their own technology device to school subject to the terms below:

Definition of Technology For purposes of BYOT

"Technology" means personally owned wireless portable electronic equipment used for instructional purposes. All approved devices must allow access to the Internet through a fully functional web browser and be capable of accessing the STARS staff/teacher network. Recognizing the rapidly changing world of technology, the list of allowed devices will be reviewed annually. Approved devices include: smartphones, iPads and other tablet computers, laptops, netbooks, and eReaders that meet the definition of "technology".

Internet

All Internet access shall occur using the STARS teacher/staff network. Security and Damages Responsibility to keep privately owned devices secure rests with the individual owner. STARS's IT department is not liable for any device stolen or damaged on campus. If a device is stolen or damaged it will be handled through the school administrative office in the same manner as other personal items that are impacted in similar situations.

Faculty and Staff Agreement

The use of personal technology to provide educational material is not a necessity but a privilege. When abused, privileges will be taken away. When respected, privileges will benefit the learning environment.

Teachers and staff participating in BYOT must adhere to all diocesan policies and the STARS Acceptable Use, Media Release and Internet Safety Procedures. Additionally:

- Teachers/Staff take full responsibility for personal digital devices at all times. The school is not responsible for the security of the device.
- The device must be in silent mode while on the school campus unless otherwise directed by or arranged with STARS administration.
- The device may not be used to record, transmit, or post photographic images or video of a person or persons on campus during school activities including STARS provided transportation and/or hours unless assigned by the administration as allowed by the STARS Acceptable

Use, Media Release and Internet Safety Procedures.

- The device may only be used to access files or internet sites which are relevant to the classroom curriculum. Non-instructional games are not permitted.
- Teacher / Staff acknowledge and agree that:
    - The school's network filters are applied to the STARS teacher/staff network Internet access and shall not be circumvented. The STARS teacher/staff network access is the only Internet access allowed for teachers and staff.
    - Under the direction of the administration, the school IT may collect and examine any school device at any time for the purpose of enforcing the terms of this agreement, or, to investigate, with reasonable suspicion, the violation of a school rule or law.
    - Teachers/Staff must not save or record (video tape) any school document or facility on his/her personal device without written authorization of school administration.

iii. Internet Safety, Social Media

Internet Safety

Teachers and Staff have the responsibility to navigate the Internet safely. All teachers and staff will participate in annual professional development in Internet safety, the management and use interactive whiteboards and mobile devices in the classroom, and an awareness training program. This professional learning will help staff and teachers to help students and families navigate conversations about digital citizenship for minors. This agreement is inclusive of an associated parent Internet safety awareness video. The school will use existing avenues of communication to further inform parents about Internet safety.

The STARS Internet safety policy is reviewed annually.

Social Media

Professional social media should be designed to support reasonable instructional, educational, or extracurricular programs under the direct supervision of STARS administration. STARS employees are responsible for their own behavior and will be held accountable for the content of the communications they post on social media sites. STARS staff who choose to engage in any type of social media should maintain a clear distinction between personal and professional social media accounts. Teachers should not ordinarily be engaged with STARS parents via social media platforms.

Professional Use of Social Media

- STARS teachers and staff should treat professional social media and communications like a professional workplace. The same standards expected in STARS professional settings are expected on professional social media sites.

- The professional social media presence should utilize the STARS email address and should be completely separate from any personal social media presence. Employees should not use their personal email address for professional social media activities.
- All professional social media accounts will be associated with diocesan provided and/or managed login credentials and privacy settings.
- Users that establish a username and password using STARS account information for any STARS approved social media/online subscription for use in the school or classroom shall provide their username and password to STARS administration and administer the resource as any other professional social media.
- All social media tools must be vetted by the STARS administration prior to use by a STARS staff member and/or teacher.
- Staff using professional social media under a STARS account have no expectation of privacy with regard to their use of social media.
- Staff and teachers are responsible for protecting confidential information. No personally identifiable student information may be posted on professional social media sites, including student photographs or video, without written consent of the students' parents/guardians.
- Staff and teachers have an individual responsibility to understand the rules of the social media being used and act to ensure the safety of students. Staff and teachers are responsible for reporting the use of social media not adhering to this agreement to STARS administration.

Personal Use of Social Media

- While the STARS recognizes that during non-work hours teachers and staff may participate in online social media, teachers and staff should keep in mind that information produced, shared and retrieved by them may be subject to diocesan policies and is a reflection of the school community.
- The personal social media presence should utilize the employee's personal email address and should be completely separate from any professional social media presence. Teachers and Staff should not use their STARS email address for personal social media accounts.
- STARS teachers and staff should not communicate with students who are currently enrolled in STARS on personal social media sites, with exceptions being made in the case of a relative. If a teacher and or staff member receive a request from a current STARS student to connect or communicate through a personal social media site they should refuse the request and report to STARS administration.
- Teachers and staff should not tag other diocesan employees, diocesan volunteers, vendors, or contractors without prior permission of the individuals being tagged.

- Teachers and staff should not use the diocesan or STARS logos in any posting and should not conduct school business on personal sites without written permission from the STARS administration.
- Teachers and staff should not access their personal social media accounts during the workday with the exception of personal break times.
- Personal social media use has the potential to result in disruption in the workplace and can be in violation of school or diocesan policy and law. In this event, administration may have an obligation to respond and take appropriate action, including but not limited to investigation and possible discipline.

2.- **Student Compliance**

i. Student Compliance

In an effort to align the new development of education and to ensure student mastery of 21st century skills, STARS provides the use of laptops, iPads, and Chromebooks, as well as email and network access to students. Therefore, all students must comply with the Diocesan Education policy, the Acceptable Use, Media Release, Internet Safety Guidelines, and the STARS Computer Guidelines.

Students who wish to have their photographs, names, or work posted on the STARS website or other publications and media must first provide consent to the Acceptable Use Policy signed by a parent/guardian.

Students shall report to school personnel any personal electronically transmitted attacks in any form made by others over the Internet or local network using any STARS technology. Students shall understand that information obtained via the Internet may or may not be correct or accurate.

ii. Internet Safety and Social Media

STARS students are responsible for their own behavior when communicating on social media. They will be held accountable for the content of the communications posted on social media sites. Students should understand and recognize that they are creating a digital footprint that could remain with them beyond their elementary school experience with potentially permanent and irreversible consequences.

- Students should exercise caution when they use exaggeration, humor, explicit language, and characterizations in all online communication.
- Students should not use the Diocese of Arlington or STARS logos in any posting without written permission from STARS administration.
- Students participating in any social media site are not permitted to post photographs of other students or STARS employees taken at school without permission from a teacher or STARS administrator.
- Students should always protect their privacy and the privacy of others. Students should not give out any personal information online.

- Students should not utilize personal social media accounts or unapproved social media sites during the school day or on school devices.
- Personal social media use, including use outside the school day, has the potential to result in disruption in the classroom. Students are subject to consequences of non-educational use of social media during the school day, and for any use of social media that disrupts or could be reasonably expected to disrupt the work and discipline of the school or classroom.

iii. Use of STARS Email (GMAIL) via Google Apps for Education

Students in grades 3-8 will be issued a Google Apps for Education account for the purpose of completing school work. Accounts may include access to Mail, Drive, Calendar, Docs, Sheet, and Slides within the STARSVA.org domain. Student mail accounts may be monitored for non-investigatory purposes and may be searched upon reasonable suspicion of a violation of law, violation of school rules, or breach of this agreement. The provided mail account is the only student mail that may be used for communication by students for instructional purposes.

Students must use appropriate language in all communications. The use of profanity, obscenity, and offensive or inflammatory language is strictly prohibited and will result in disciplinary action. Instruction on safe and appropriate use will be provided.

By default, users with Gmail (Business and Education) accounts at any domain can send mail to and receive mail from any other email address. However, STARS will restrict the student email addresses to exchange mail within the STARS domain only. In this way, STARS students will have access to exchange mail with the teachers, faculty, and other students, but not with people outside of the STARS Domain.

Students who attempt to send mail to a domain not listed will see a message that specifies a policy prohibiting mail to that address, confirming that the mail is unsent. Students will receive only authenticated messages from within the STARS domains. Messages sent from outside of STARS domains will be returned to the sender with a message about the policy.

3.- **Network Security**

These policies apply to everyone at STARS. STARS provides additional details on how to be compliant with the policy, and the policy should be used as a normal part of daily life at STARS in order to keep both STARS confidential data and the user's own personal information secure.

i. Users:

- Only users with valid STARS network accounts are authorized to use the STARS network and computer equipment. Employees and students must only use their assigned network account. Employees and students are prohibited from giving anyone their network password or network account information other than to an authorized IT or Instructional Technology personnel.

1. *Password Management*

- User passwords and other access credentials must never be shared.
- All passwords and other access credentials must be protected.
- Different passwords must be used for STARS and non-STARS accounts.
- Passwords used on all systems for STARS business should be of sufficient length and complexity to reasonably protect them from being guessed by humans or computers.
- Passwords must be changed immediately if there is suspicion of compromise.
- Confidential information must only be accessed for authorized purposes.
- Confidential information must only be shared with those authorized to receive it.
- All devices (including desktops, laptops, and mobile devices such as smartphones and tablets) storing or processing confidential information must meet STARS device protection requirements.
- Information such as students' grades and records must not be stored on personal user devices or portable media unless the device or media is encrypted.
- Information such as medical records may only be used, stored, or processed on servers or services (such as file sharing or collaboration services, cloud-based email services, cloud-based backup and recovery services, etc.) that meet applicable STARS data protection requirements.

2. *Protecting Confidential Information*

- Confidential information in any form must be appropriately protected.
- Confidential information in any form must be appropriately disposed of when it is no longer needed.
- Any actual or suspected loss, theft, or improper use of or access to confidential information must be reported promptly.
- All users handling credit or debit card transactions must comply with STARS Management requirements.

3. *Devices*

- All devices must be configured for secure storage, transport, and disposal of confidential information. Review checklists for secure configuration of your device type.
- All user devices must be configured for secure operation. The device must be configured to limit access to the specific person or persons authorized to use the device.

- The information stored on the device must be protected against access if the device is lost or stolen.
- Operating system and application patches must be applied promptly.
- Client applications on the device which might be used to access or transfer confidential information must be configured to protect their communications.
- The information stored on the device must be protected against access when the device is disposed of.
- Any actual or suspected loss, theft, or improper use of a device storing confidential information must be reported promptly.

- No alternative network shall be created or used by any staff or student unless approved by the IT Department. “Alternative network” is defined as any wired or wireless network or sub-network located on or accessible from any STARS property that is not part of the primary network managed by the IT Department. All network equipment must be installed and/or approved by IT Department staff.
- Students may not allow another user access to use a computer while logged in. All computer users should always lock or logoff from the network before leaving their room or office.

ii. *Devices*

- For the protection and security of STARS data, all computers attached to the STARS physical network (a computer located at a STARS facility either wired or wireless), must be the property of STARS. A computer that is not property of STARS may not be attached to the network without first receiving a written approval from the administration to do so.
- Use of software designed to gain passwords or access beyond the rights assigned to a user or computer is strictly prohibited. Use of such programs risk the security of the network and is considered "hacking". Such unauthorized access is a violation of State and Federal law. Violators will be prosecuted. Should an employee or student inadvertently discover passwords or any other measure used to obtain unauthorized access, they must report it to the IT Department.
- No user shall encrypt files or folders or attempt to hide files or folders stored on a network server or local workstation unless written approval is granted by the administration and IT Department.
- All network user accounts may be monitored for non-investigatory purposes, and may be searched upon reasonable suspicion of a violation of law, violation of school rules, or breach of this agreement.

4.- **Network Drives / Share**

Network drives have been provided to all users for the ease of use of network resources. Drive letters assigned to an authorized network user are specific to that individual user. Any attempt to gain access to a drive that is not assigned to a user account is strictly prohibited. The unauthorized examination of information stored on a computer system or sent electronically over a network is a breach of academic and community standards. Authorized staff however, may gain access to users' data or programs when it is necessary to maintain or prevent harm to the school, its computer systems or the network.

On shared and networked computer systems certain information about users and their activities is visible to others.

All STARS users have the legal obligation to maintain the privacy of files containing confidential information, including student information such as course grades.

All teachers, staff, and authorized users have access to a Public Folder on the server. This is the "S" drive. Please use it with caution as anyone can read and only authorized users may delete information in this directory.

5.- Saving Documents, Naming Conventions, and Virus Protection

Saving Documents

Employees and students may save documents to the network but shall not save any applications to the network without authorization described herein below. Due to server storage limitations, any applications or executables residing in a user directory will be deleted. (Exception is given where individuals have created applications as part of a curriculum assignment and such activity has been approved by a member of the STARS Administration.) Any document with a Virus will be deleted permanently from the network without exception.

Document Naming Conventions for a Shared Network Drive--Recommendations

- Create unique file names. Duplicate file names will cause problems.
- File names should be simple and easy to understand.
- Use only alphanumeric characters. DO NOT use special characters such as: ? / $ % & ^ # . \ : < >.
- Avoid the use of underscores (_) and dashes (-) to represent spaces.
- Use leading zeros with the numbers 0-9 to facilitate proper sorting and file management.
- Dates should follow the standard of YYYYMMDD. This maintains chronological order. If dates of creation are used, these can make following retention schedules easier.
- Keep the file name as short as possible and always include the three character file extension preceded with a period (Ex: .jpg or .doc).
- Include the version number in the file name by using 'v' or 'V' and the version number at the end of the document. (Ex: 2004_Notes_v01.doc) Avoid using the word version or draft and the beginning of the file name for access purposes (Ex: Version1_2004_Notes.doc).
- Order the pieces of information or elements being used to create the file name

in the most logical order based on retrieval methods. For example, use the date first on events that are time specific or recurring, and use the name of the event for events that are infrequent and will be easier to find by name rather than date.

Virus Protection

- The STARS IT Department will provide all virus protection and related software for all laptops, workstations, and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the STARS administration.
- Users should never open any email attachments from an unknown sender. Never send an email suspected of containing a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted. Contact the IT Department immediately to report a computer that may contain a virus.
- There are many virus tricks. Never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to make sure the virus is valid and not a trick.
- No student or employee is allowed remote access (access from outside the STARS network) to any STARS network resource from a non-STARS computer without first obtaining a working and updated virus protection program. This includes, but is not limited to, VPN Access.

6.- **Computer and Laptop use**

- All teachers, staff, and students are prohibited from installing any software on any computer unless authorized in writing by a member of the IT Department. Illegal downloads or use of copyrighted software, music, videos, pictures, or other files is strictly prohibited. Only compatible, legitimate, and approved school related software is acceptable.
- All employees and students are prohibited from using any STARS computer for illegal, obscene, pornographic, personal profit, or commercial activity.
- Changing or tampering with any computer's system configuration is strictly prohibited.
- Any attempt to bypass the internet content filtering by use of a proxy or other means is strictly prohibited unless authorized by the IT Department. Content is filtered for all users accessing the Internet through the STARS network.
- Any desktop applications designed to limit access to students or staff, other than those used by the IT Department for network security purposes, is prohibited.
- Use of a broadcast messenger service such as "net send" to send messages over the network is prohibited except in the case of an emergency.
- Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.
- No computer shall be moved by anyone other than IT Department personnel

unless approved by a member of the IT Department.

7.- **Copyright Policy**

- STARS reserves the right to monitor employee computer systems (including desktop, laptop, and handheld devices) and any content stored on an employee's computer system.
- STARS also reserves the right to remove, delete, and modify or otherwise disable access to any materials found to be infringing of copyright.
- Any shareware or software to be used on STARS computers should be licensed by STARS if they are to be used by an employee, consultant, or contractor. For the security and safety of our systems they should also be installed with the permission and assistance of the IT Department. Employees are reminded that all computers, equipment, and software supplied by STARS are subject to periodic audit.
- If an employee is issued a password to access information licensed by STARS the employee is expected to take all reasonable measures to protect the security of the password and not to share the password with anyone.

8.- **E-mail / Communication**

E-mail

The STARS e-mail system has been provided for the internal and external communication of staff, teachers, and students. The e-mail system may not be used for personal gain or political or religious views (contrary to the teachings of the Catholic Church), or in any illegal, offensive, or unethical manner. The e-mail system is intended only for valid and legitimate STARS related communication.

STARS reserves the right to access any e-mail for business purposes and also for inspection for disciplinary or legal actions.

STARS' staff and teachers must NOT send text messages to a student from personal devices. Teachers must use a STARS email to contact students or parents.

Electronic Communication

All communication conducted electronically between a STARS teacher, staff, and a student shall be for the purpose of official business of STARS. STARS staff must not initiate email to students unless the staff has a written permission from the parent/guardian upon approval of the school principal. Email messages should be generated by the teacher from a STARS email account. STARS teachers must complete STARS training before establishing communication with students. Email communication from a STARS faculty or staff member to a student shall only be through the faculty/staff member's STARS email account and the STARS student email account.

PARENTS--ACCEPTANCE OF TERMS AND CONDITIONS:

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties.

I have read this policy and understand that the school wishes to expand the availability of information to students and at the same time attempt to assure the appropriateness of this information as it relates to the goals of the school. By signing below, I give permission for the school to allow my son or daughter to have access to the Internet and other technology resources under the conditions set forth above.

Parent or Guardian Name (Please Print)   Parent or Guardian Signature   Date

Student(s) Name(s) (Please Print)