Internet Safety and Acceptable Use Policy (ISAUP)

14-2015 Revision List

1. Replaced all instances of Internet Safety and Acceptable use policy with ISAUP.
2. Replaced all instances of email, and chat logs with electronic communication.
3. Added scope of policy and condense Opportunities and Risk of Technology Use
4. Added community to all relevant sections
5. Added Internet filter and liability section
    a. Added filtering review section
    b. Added lost, stolen, or damaged personal technology statement
6. Privileges and Responsibilities section, use of technology will
    a. Moved E-discovery statement to Logging, monitoring, and data retention section
    b. Removed old #5 “Be responsible at all times with the proper use of technology including the proper use of access privileges, complying with all system security identification codes, and not sharing any codes or passwords” - Redundant.
    c. Added #7 “Report intercom or phone issues immediately. This only applies to faculty/staff.”
7. Privileges and Responsibilities section, use of technology will not
    a. Made #2 more broad
    b. Added #3 “Use a personal or school provided device on school grounds or a school-related function (a) with the intent to intimidate, harass, coerce another person, or (b) to use vulgar, obscene, profane, lewd, or lascivious language to communicate such harassment, or (c) to threaten an illegal or immoral act.”
    c. Moved old #4 to #18 and cleaned up language
    d. Combined old #6 and #7 into new #5
    e. #7 - added “or forge electronic materials”
    f. Removed old #10 “Use the network to distribute or share files (including music and video files), images, applications, etc. with others unless the user has received direct permission from the author and appropriate teacher to do so and the material is not copyrighted.” - redundant as copyright laws and fair-use covers this.
    g. #11 - added without permission - for our cyber challenge competition participants
    h. Old #17 is now #14 - changed sign in page to BYOD initiative
    i. Added #20 - Covers defacing equipment
    j. Removed old #21 - redundant with #1
    k. Added #21 - “Disconnect, disable the ringer, unplug or tamper with any school phone.” - safety and security
8. Changed heading from “Wireless networking, laptops, and other portable communication devices” to “Bring your own device “BYOD” initiative”
    a. Changed “No assistance besides the information provided on the I.T. site will be provided for anyone connection a personal device to the ARGS provided wireless network.” to “ARGS I.T. is under no obligation to provide any assistance to any personal device at any time.”
    b. Added “This is an optional initiative: No student or faculty/staff member will be required to bring their own device. BYOD devices are the sole responsibility of the

person bringing them. Computer are provided at the campus at a ratio of 2 computer to every 1 student.

9. Rewrote Electronic Communications section
10. Added new section “Electronic Trust relationship” - to protect school integrity
11. Physical Technology equipment section
    a. added “All computer equipment and accessory purchases using school appropriated funds must be approved by the ARGS I.T. department for compatibility with our network. ARGS I.T. maintains a list of approved equipment”
12. Reporting violations section
    a. Added “Students should report any cyberbullying to a school administrator immediately.” - Cyberbullying
13. Added logging, monitoring, and retention section
14. Under the Disciplinary Action section
    a. Added “If equipment is purposefully defaced, destroyed, or damaged that person will be responsible for the full replacement value for the equipment.”
15. New signature page

Technology Use

Appomattox Regional Governor's School provides access for students, staff, and its community to resources from around the world through an electronic communication system which includes internet and electronic communication access. All uses of the ARGS computer system, including Internet access, must in support of education and/or research, or legitimate school business.

Unless otherwise specified this policy only applies to the use of any ARGS technology equipment, Internet/Network access provided by ARGS technology equipment, or services provided by ARGS.

The Opportunities and Risks of Technology Use

The Appomattox Regional Governor's School believes that the value of information and interaction that technology offers outweighs the possible hazards of its use. Making network, internet and electronic communication access available to students, staff, and the community, however, carries some risk to the users and to the security of personal information. Because information on networks is transitory and so diverse, ARGS cannot completely predict or control what users may or may not locate either intentionally or accidentally.

Internet filtering and liability

In accordance with the Children's Internet Protection Act (CIPA) , VADOE Policy: 1.75 – Use of Electronic Communications And Social Media, the Keeping the Internet Devoid of Sexual Predators Act of 2008 (42 USC 16901 § 431), Protecting Children in the 21st Century Act, and the Family Involvement in Technology (FIT) Program (Code of Virginia § 22.1-212.2:3), ARGS installs, operates and monitors filtering software to limit users' internet access to materials that are obscene, pornographic, or harmful to children, or otherwise inappropriate, notwithstanding that such software may at certain times block access to other materials as well.

At the same time ARGS cannot guarantee that filtering methods will in all instances successfully filter access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate. The use of Internet filtering does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials. No technology is guaranteed to be error-free or totally dependable. Among other matters, ARGS, ARGS I.T. department, ARGS administrative team and the school board is not liable or responsible for:

- any information that may be lost, damaged, or unavailable due to technical or other difficulties
- the accuracy or suitability of any information that is retrieved and/or produced through technology, breaches of confidentiality, or defamatory material.

- breaches of personal security as a result of user error, weak user password, or a security vulnerability.
- access to material that may be seen as offensive or obscene in nature as a result of a system failure or system bypass either accidently or intentionally.
- Lost, stolen, or damaged personal equipment.

ARGS I.T. reviews the filtering methods annually and evaluates the current filtering solution to newer solutions. Filtering software is selected based on its effectiveness, stability, ethical standards, speed, and transparency.

Privileges and Responsibilities

The Appomattox Regional Governor's School's network is a part of a curriculum and is not a public forum for general use. Users may access technology only for educational purposes. Access to the ARGS network "the Network" and use of the technology related equipment is a privilege, not a right. We will strive to provide equitable opportunities for the use of technology, and the I.T. department will take reasonable measures to inform students and staff of the rules and regulations regarding network and equipment use in staff and student handbooks. This policy shall apply to all users and devices including but not limited to faculty, students, administrators, staff, community, and guests.

Users of technology will:

1. Comply with copyright laws, fair-use laws, and software licensing agreements.
2. Respect the privacy rights of others and maintain confidentiality of all personnel and student records stored.
3. Make a best effort to maintain the integrity of technological resources from potentially damaging messages, physical abuse, viruses, malware, scams, and phishing schemes.
4. Respect the rights of others to use equipment.
5. Recognize that there is no assurance of confidentiality with respect to sent or received communication(s).
6. Understand that a third party may have access to the user's data only through the I.T. department for the sole purpose of off-site backups, remote administration/technical support, or remote hosted/cloud applications.
7. Report intercom or phone issues immediately. This only applies to faculty/staff.

Users of technology will not:

1. Access, submit, post, publish, display or create any content that is defamatory, intentionally misleading, abusive, obscene, profane, sexually oriented, threatening, harassing, or illegal.
2. Use the provided technology resources for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If a student inadvertently accesses such information, that student should immediately disclose the inadvertent access to a teacher or other school official. Other authorized users should report the incident to the Network Administrator.
3. Use a personal or school provided device on school grounds or a school-related function

(a) with the intent to intimidate, harass, coerce another person, or (b) to use vulgar, obscene, profane, lewd, or lascivious language to communicate such harassment, or (c) to threaten an illegal or immoral act.

4. Interfere with, or disrupt the Network use by others; create and/or propagate unsolicited advertising, chain letters, pyramid schemes, computer worms, viruses, or other acts of vandalism. Vandalism includes any attempt to harm or destroy data of another user, the Internet, the Network or any other network. Vandalism includes knowingly transmitting a computer contaminant, or inserting a computer contaminant into a computer, computer program, computer software, or network of another without the knowledge or permission of the owner of that computer, computer program, computer software or computer network.
5. Use another's account credentials or distribute user credentials without the permission of the I.T. department.
6. Knowingly distribute plagiarized material.
7. Misrepresent themselves or forge electronic materials.
8. Trespass in others' folders, work, or files, or attempt to gain unauthorized access to resources or entities.
9. Violate the Family Educational Rights and Privacy Act (FERPA).
10. Use ARGS technology services for non-school related purposes.
11. Attempt to breach and/or breach security measures or remove hardware/software, networks, information, or communication devices from any network without the permission of the owner of that computer or computer network.
12. Use the network while access privileges are suspended or revoked.
13. Use the telephone system unless previously authorized by a teacher, staff member, or administrator to do so.
14. Use any unauthorized personal equipment to attach, connect to or install on the Network with the exception of any device using our BYOD initiative.
15. Intentionally disrupt the network by any means with any type of hardware or software.
16. Maintain or use an account that has heightened privileges to install or modify a computer/device that is owned and operated by Appomattox Regional Governor’s School without the permission of ARGS I.T.
17. Use any form of electronic communication (either provided by ARGS or provided by an external source) for the sole purpose of soliciting sexual contact or romantic relationship with a student.
18. Send mass electronic communications which serve no academic or administrative purpose, such as chain letters. Students must seek prior approval before sending any mass communications.
19. Make changes in the physical setup of any technology device owned by ARGS unless approved by the Information Technology Department. Examples include, but are not limited to: removing or disconnecting any peripherals connected (such as the mouse, keyboard, or speakers) or disconnecting a device from the local area network. USB hard drives and USB memory sticks are exempt from this.
20. Permanently write on, deface, destroy, or damage technology equipment for any

purpose. All technology equipment purchased with school appropriated funds belongs to the organization ARGS, not a specific department or person.

21. Disconnect, disable the ringer, unplug or tamper with any school phone.

Bring your own device "BYOD" initiative

Users may not connect to any other wireless network except the ARGS Wireless Network while on-campus. This includes wireless internet access by cell carriers and access points maintained by the residences adjacent to the property. Any user found to be accessing the internet on a personal device without express permission by a teacher, administrator, or the I.T. Department will be subject to the disciplinary actions set forth in this policy.
Access to the Wireless Network may be restricted to a per-user basis. Anyone who is authorized for wireless access to the network will be subject to the rules and regulations set forth in this policy. If a user violates any portion of the ISAUP, the right to access the Wireless Network may be immediately and permanently revoked.

Students may not use laptops or portable computing/communication devices while in class without the express permission of their teacher.
It should be noted that wireless connectivity is considered a secondary network and connectivity is not guaranteed on your device. ARGS provides and maintains computers for students and staff to use.

ARGS I.T. is under no obligation to provide any assistance to any personal device at any time.

This is an optional initiative: No student or faculty/staff member will be required to bring their own device. BYOD devices are the sole responsibility of the person bringing them. Computers are provided at the campus at a ratio of 2 computers to every 1 student.

Websites and Web pages

Authorized users may create web pages only as part of a class activity. Material presented on a class website must meet the educational objectives of the class activity. The Class Sponsor/Teacher, Department Head, I.T. Department, and Administration have the right to exercise control over the content and/or style of the student web pages. All class web pages shall be posted through the school website and not housed off school grounds unless prior approval is obtained in writing.
Only those students whose parent(s) or guardian(s) have consented and signed a release may post their work or picture on student or school websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only for confidentiality and safety purposes unless otherwise approved by ARGS administration and a parent or guardian.

Guidelines for use of Electronic Communications

New technologies, such as social networking tools, blogs, forums, and message boards, provide exciting new ways to collaborate and communicate. Activities which are improper, unethical, illegal, or which cause undue discomfort for students, employees, parents, or other members of the school community should be judiciously avoided in both physical space and on the Internet.

To that end, we offer the following guidelines for school employees who use online social networking, communication methods not provided for you by ARGS and approved for education use.

1. Friending: Faculty/Staff should not initiate friend contacts with current students or accept friend requests from current students.
2. Unequal Relationships: Understand that the uneven power dynamics of the school, in which faculty and staff have authority over former students, continues to shape those relationships.
3. Privacy settings and content: Exercise care with privacy settings and profile content. Content should be placed thoughtfully and periodically reviewed to maintain this standard. Be aware that some of your communications may be public or semi-public even though your privacy settings may reflect otherwise.
4. Public Information: Recognize that many former students have online connections with current students, and that information shared between school adults and former students is likely to be seen by current students as well.

These applications which may be frequented by current students, former students, and potential future students. The incorrect use of these applications can have a negative impact on the school, school board, community, students both current and future, and yourself. Exert an extreme amount of caution while using these services. Use of applications and communication methods not approved for your use with ARGS students or education use should be avoided in most cases.

Electronic Trust Relationship

ARGS maintains a number of resources for students, parents, board members, and community members. All users of this content should understand how to find information on the public Internet that is accurate.
Please use the following guidelines to ensure you are getting accurate information:

- Only websites linked on the ARGS website (https://www.args.us) are considered to be endorsed by the school. Sites claiming to be ARGS related but not linked on the ARGS website should be viewed as a personal opinion and may not express the thoughts and opinions of the Appomattox Regional Governor's School. Your browser must say the connection is secured and is pointed at https://www.args.us or a sub-domain of args.us (e.g. https://powerschool.args.us) to ensure the trust relationship.
- ARGS does not maintain a public social networking presence; all postings found on social media are personal in nature and do not reflect the thoughts and opinions of the Appomattox Regional Governor's School.
- Most wiki style sites can be changed at any time by almost any person.

Physical Technology Equipment

The ARGS I.T. Department cannot be held responsible for any equipment that was not directly purchased by the Appomattox Regional Governor's School. Equipment not purchased by the Appomattox Regional Governor's School will not be serviced by the ARGS I.T. department. All computer equipment and accessory purchases using school appropriated funds must be approved by the ARGS I.T. department for compatibility with our network. ARGS I.T. maintains a list of approved equipment.

Reporting Violations

Any actual or suspected violation of the rules listed in the ISAUP must be brought to the attention of the Information Technology Department immediately. The Information Technology Department will perform an investigation and determine the appropriate course of action with the assistance and support of ARGS Administration.

Students should report any cyberbullying to a school administrator immediately.

Logging, monitoring, and data retention

All users must understand that electronic communication, internet usage and network files are not private. All electronic transactions may be logged in accordance with the Electronic Discovery Act. Several systems are in place to keep ARGS systems compliant.

The following resources are logged:

- All electronic communication system access provided by ARGS, this includes emails, chats, comments on documents, and
- Webpages visited by a user, DNS record accessed, and IP addresses accessed.
- Documents created, modified or deleted. This may be limited to metadata only.
- Security events from any system attached to the network.
- Access attempts to our website(s).

Monitors

- Network traffic is regularly monitored by the I.T. department in an effort to maintain network integrity as well as ensure that traffic is educational in nature.
- Security events are regularly monitored to ensure the safety of all user accounts.
- Certain triggers are put on all email accounts for keywords and are monitored by the ARGS I.T. department

Data retention

- All data will be retained for the minimal listed by the Library of Virginia or 10 years whichever is greater.
- Under *Code of Virginia* § 42.1-85, the Library of Virginia (LVA) has the authority to issue regulations governing the retention and disposition of state and local public records. In keeping with the Code's mandate, LVA has developed Records Retention & Disposition

Schedules outlining the disposition of public records (http://www.lva.virginia.gov/agencies/records/retention.asp).

E-Discovery requests can only come from the ARGS Executive Director or litigation.

ARGS Response to a Reported Violation

Upon receipt of a violation notice, ARGS I.T. may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings. A person accused of a violation will be notified of the charge and have an opportunity to respond before ARGS imposes a permanent sanction. If a user is deemed to be in violation of the ISAUP, that student will be subject to the disciplinary actions defined in the following section.

Disciplinary Action

Failure to observe the ISAUP will result in possible disciplinary actions from the ARGS Administration. Punishment for infractions of the ISAUP includes, but is not limited to:

- a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, ARGS-administered computing rooms, and other services or facilities.
- verbal warnings
- disciplinary probation
- suspension from school
- permanent dismissal from school
- possible criminal prosecution

School administrators may impose any additional disciplinary actions not listed in this policy as deemed necessary by a situation which they feel warrants such actions.

Criminal prosecution, depending on the circumstances of each incident, may be necessary. If your activity breaks the law, you can be prosecuted. Even if you are not charged criminally, you can still be suspended from the school. Parents or guardians will be involved in any case which may result in suspension or dismissal from the school. Parents or guardians may be liable for damages resulting from student abuse of any system.

The school reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending device from the campus network, terminating a session, terminating a running job on a system, or taking other action. If ARGS I.T. believes it's necessary to preserve the availability, security, or integrity of facilities, user services, data, data security, or network security, it may temporarily suspend any account, service, or server with or without notice, whether or not the account/user is suspected of any violation. Servers, computers, and services that threaten the security of school systems may be removed from the network and allowed to reconnect only with the approval of network administration.

If equipment is purposefully defaced, destroyed, or damaged that person will be responsible for the full replacement value for the equipment.

Staff responsibilities to Students

Staff members utilizing the network, internet and/or computer resources for instructional purposes with students are responsible for supervising such use. In selecting technology for teaching purposes, staff shall comply with the selection criteria for instructional materials and library-media center materials. Staff members are expected to be familiar with the School's policies and any administrative rules concerning student computer and network use and then enforce them. When in the course of their duties staff members become aware of student violation(s), they are expected to stop the activity and/or inform the Information Technology Department.

Additional Rules/Actions/etc

- Community Outreach includes our newsletter, mailing lists, and our main website.
- ARGS offers ongoing professional development and needs assessments every year with our pre-school workweek.
- The ARGS I.T. Director will perform an annual security audit and make the necessary adjustments to ensure the safety and security of all network operations.
- All students must attend our Internet safety assembly as part of entering the school in 9th grade.
- The ARGS Administration Team may establish additional procedures and guidelines and shall take appropriate action to implement this policy as necessary.
- The school board will review, amend if necessary, and approve this policy every year.
- This ISAUP complies with all state and federal telecommunication codes, laws, and regulations.
- For questions about the Internet Safety and AUP, students should talk to an ARGS staff member, and staff members should talk to ARGS Administration or Information Technology. As always, if you don’t know, ask.

ARGS ISAUP 2014-2015 School Year.
Board Approved Date:June 2014

Each teacher, administrator, student and parent/guardian of each student shall sign the ISAUP before using the schools computer system each school year. The failure of any student, teacher or administrator to follow the terms of the Agreement, this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

By Signing this you intend to abide by the rules and restrictions as indicated in the Internet Safety and Acceptable User policy as well as all state, federal, and local laws. Where applicable, you agree to allow your child to access the Internet, network resources, and school provided electronic communications.

_____	_____
Name (Printed)	Name (Signed)
_____	_____
Date	Student Name (if parent signing)

References and Laws

VITA Security Policy
http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/unmanaged/library/psgs/Security_Policy_519_00_Final_0709.pdf

Computer fraud
18.2-152.3 § 18.2-152.3

Computer invasion of privacy
18.2-152.5 § 18.2-152.5

Computer trespass(hacking/cracking)
18.2-152.4 § 18.2-152.4

Enhanced penalties for using a computer in certain violations(advertising/producing obscene materials)
18.2-376.1 § 18.2-376.1

Harassment by computer(cyberbullying)
18.2-152.7C1 § 18.2-152.7:1

Identity theft
18.2-186.3 § 18.2-186.3

Personal trespass by computer
18.2-152.7 § 18.2-152.7

Possession,reproduction, distribution, and facilitation of child pornography
8.2-374.1C1 § 18.2-374.1:1

Production, publication,sale, financing,etc., of child pornography, presumption asto age
18.2-374.1 § 18.2-374.1

Property capable of embezzlement (by computer)
18.2-152.8 § 18.2-152.8

Theft of computer services
18.2-152.6 § 18.2-152.6

Transmission of unsolicited bulk electronic mail (spam)
18.2-152.3C1 § 18.2-152.3:1

Use of communications systems to facilitate certain offenses involving children (solicitation)
18.2-374.3 § 18.2-374.330

Guidelines and Resources for Internet Safety in Schools Using a computer to gather identifying information (phishing/pharming)
18.2-152.5C1 § 18.2-152.5:1

VDOE Internet Safety Guidelines and Resources
http://www.doe.virginia.gov/support/safety_crisis_management/internet_safety/guidelines_resources.pdf