Research Triangle High School Technology Standards, Policies & Procedures

Table of Contents

Introduction 5
General Information 5
RTHS Policies 5
Responsible Use Policy 5
Reporting Computer Problems or Requesting Technical Assistance 5
Requesting Password Resets 5
Remote Working Policy 6
Compensation and Work Hours 6
Eligibility 6
Equipment/Tools 6
Security 6
Workspace 6
Office Supplies 7
Worker's Compensation 7
Liability 7
Dependent/Child Care 7
Taxes 7
Communication 7
Problem-Solving/Policies 7
Attire/Conduct 7
Tracked Time Worked 7
Time off/Leave/Sick Time 8
Hardware 8
Hardware Purchasing Standards 8
Electronic Equipment - School Purchase 8
Inventory 8
Computer Repair 9
Relocation of Equipment 9
School-Based Programs Involving Technology 9
Computer Donations 9
Acquiring Technology by Grant or Crowd Sourced Funding 9
Employee-Owned Hardware 10
Checkout of Technology 10
School-Owned Hardware Use 10
Technology Life Cycle Replacement Plan 10

Introduction....10
Principle/Goals....10
Hardware Platforms....11
Life Cycle Equipment Replacement Term....11
Equipment Assignment....11
Responsibilities of RTHS Personnel Receiving Equipment....11
Default Equipment....12
Exceptions to the Standard Build and Configurations....12
Exception Approval for Apple/Mac Devices and Rational for Deviation....12
Retirement of Equipment....12
Software....12
Standard Software....12
Personally Owned Software....13
Network Access/Email....13
Network Access Policy....13
Purpose....13
General....13
Management Responsibilities....14
Audit Controls and Management....14
Security....14
Technology Security....14
Procedure....15
Definitions:....15
Security Responsibility....16
Training....16
Physical Security....16
Computer Security....16
Server/Network Room Security....17
Contractor access....17
Network Security....17
Network Segmentation....17
Wireless Networks....17
Remote Access....18
Access Control....18
Authentication....18
Password Creation....18
Password Protection....18

Authorization....18
Google Vault Authorization....18
Accounting....18
Administrative Access Controls....19
Incident Management....19
Business Continuity....19
Malicious Software....19
Internet Content Filtering....19
Data Privacy....20
Security Audit and Remediation....20
Enforcement....20
Establishing Network Access and Email Accounts for Employees....20
Name Changes for Network Access and Email Accounts....21
Closing Accounts for Retirements, Resignations or Terminations....21
Establishing Network Access and Email Accounts for Non-Employees....21
Requesting Password Reset....21
Security Policy....21
Filtering and Access to Information....22
Personal Use of Email....22
Management of Email Accounts....22
Mass Distribution of Email....22
Release of Email Addresses....22
Confidential Information and Use of Email....22
Privacy of Email/Calendars....22
Surveillance Camera Policy....23
Purpose of Surveillance Cameras....23
Monitoring....24
Storage....24
Release of Information....24
Destruction and/or Tampering with Surveillance Cameras....24
APPENDIX A....25
Expectations for Technology Security....25
APPENDIX B....26
Acceptable Use of Technology....26
Network Etiquette....26
Email....27
Passwords....27

Copyright....27
Security....27
Plagiarism....27
Vandalism....27
Network resources....27
Emerging Technologies....28
School Issued Technology....28
Web 2.0/Social Networking Tools:....28
Internet Safety and Children's Internet Protection Act (CIPA) and Research Triangle High School Student Email Accounts....29
Access to Inappropriate Material....29
Inappropriate Network Usage....30
Education, Supervision and Monitoring....30
APPENDIX C....31
Troubleshooting....31

Introduction

All technology resources employed by Research Triangle High School should be used in a responsible, legal and ethical manner. To encourage responsible and ethical behavior, guidelines for using these resources must be instituted. The guidelines must safeguard students, protect the school and its staff from liability and protect the school's investment in technology.

RTHS Acceptable Use Policy (AUP) ensures the uses of technology are consistent with the goals of the school. The AUP states that the technology department is responsible for establishing standards, policies, and procedures related to the use of technology in the Research Triangle High School.

The Technology Policies, and Procedures was written to further outline the School's responsible use of technology. The procedures and standards outlined in this document have been developed by the technology department. The goal is to provide a standard and controllable network environment for the school. The technology department is charged with reviewing, approving and setting standards for all hardware, software and network access.

This document includes important guidelines such as repair of equipment, purchase of software, acceptance of donated equipment, requests for technology services that are listed in this document may be submitted to the technology department (tech@rthighschool.org). Any application not included in this document requires review and approval of the technology department.

General Information

RTHS Policies
Research Triangle High School's internet connection has been established in the belief that the information and interaction available are valuable additions to educational resources. All technology resources employed by RTHS must be used in a responsible, legal and ethical manner. RTHS Responsible Use Policy ensures the uses of technology are consistent with the goals of the school.

Responsible Use Policy
The Acceptable Use Policy addresses:

1. Acceptable Use
2. Personal Responsibility
3. Network Etiquette
4. Passwords
5. Copyright
6. Security
7. Plagiarism
8. Vandalism

The Acceptable Use Policy is included in the Student Handbook. The Student Handbook includes a Code of Conduct that outlines proper conduct and behavior of students and disciplinary consequences. Each student is required to provide a copy of the Code of Conduct to his or her parent/guardian and every student and parent/guardian will sign as verification that they have reviewed the handbook and understand the consequences.

Reporting Computer Problems or Requesting Technical Assistance

Requests for computer repairs, relocation of equipment, email problems, printer problems, software or hardware installations, etc., should be submitted to the IT department (tech@rthighschool.org).

Only the technology department or office manager has the authorization to schedule an outside service to come fix equipment. (Printers, Network, Phone System, etc.)

Before submitting a request, the following may be helpful:

- ✓ If you are having computer problems, refer to the Troubleshooting Guide in Appendix C.
- ✓ If the issue is urgent and needs to be resolved in an immediate manner, then please use Tech Support Google Chat Space. If it is non-urgent, then please email tech@rthighschool.org
- ✓ If you determine you need technical assistance, report the problem in as much detail as possible.

Requesting Password Resets

Staff/Faculty/Student Passwords: Requests for password resets (Google Workspace, PowerSchool, or school computer logins) can be made to tech@rthighschool.org . Depending on the platform and availability, self service password requests can be made with your school assigned email address as well.

Remote Working Policy

To maintain efficient and safe operations and to encourage employees to give their full attention to their dues during this unusual time, RTHS will allow certain employees the opportunity to telework. Remote working is the concept of working from home or another location on a full- or part-time basis. Remote working is not a formal, universal employee benefit. Rather, it is an alternative method of meeting RTHS's needs during unusual times. Indeed, Remote working, especially for teachers and instructional staff, is not ideal and will not be permitted absent extraordinary circumstances such as the current health crisis. RTHS has the right to refuse to make remote working available to an employee and to terminate a remote working arrangement at any time in its sole discretion.

Compensation and Work Hours
The employee's compensation, benefits, work status, and work responsibilities, will not change when remote working unless an employee is notified in writing of such change. The amount of time the employee is expected to work per day or pay period will not change as a result of teleworking. However, schedules and hours may change depending on RTHS's needs and expectations.

Eligibility
Successful remote workers have the support of their supervisors and RTHS leadership. Not all employees will be eligible to work remotely. RTHS shall provide training and instructions for remote working.

Equipment/Tools
RTHS may provide specific tools/equipment for the employee to perform his/her current duties. This may include computer hardware, computer software, phone lines, email, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary. The use of equipment, software, data supplies and furniture when provided by RTHS for use at the remote work location is limited to authorized persons and for purposes relating to School business. RTHS will provide for repairs to company equipment. When the employee uses her/his own equipment, the employee is responsible for maintenance and repair of equipment. A loaner laptop may be provided when available. Loaner computers will vary in performance and configuration. Loaners must be returned upon request.

Security
RTHS expects all telecommuting employees to comply with the Guidelines set out in Appendix A regarding technology security.

Workspace
The employees shall designate a workspace within the remote work location for placement and installation of equipment to be used while teleworking. The employee shall maintain this workspace in a safe condition, free from hazards and other dangers to the employee and equipment. The workspace shall be professional, appropriate and conducive to audio and visual interactions with students, families and co-workers. Employees are expected to submit three photos of the home workspace to their supervisor prior to implementation of teleworking.

Any School materials taken home should be kept in the designated work area at home and not be made accessible to others. This is particularly important when such materials include student and/or family

information or other information that could be deemed confidential. RTHS has the right to make on-site visits (with 48 hours advance notice) to the remote work location for purposes of determining that the site is safe and free from hazards, and to maintain, repair, inspect, or retrieve School-owned equipment, software, data or supplies or to ensure that the employee is complying with School policies.

Office Supplies
RTHS will provide any needed office supplies. Out-of-pocket expenses for other supplies will not be reimbursed unless prior written approval of RTHS in accordance with its fiscal policies.

Worker's Compensation
During work hours and while performing work functions in the designated work area of the home, telecommuters may be covered by worker's compensation.

Liability
RTHS is not liable for loss, destruction, or injury that may occur in or to the employee's home. This includes family members, visitors, or others that may become injured within or around the employee's home.

Dependent/Child Care
RTHS recognizes the challenges during this difficult time. However, it is important that employees prioritize and perform their work while remote working. This means that remote work is not a substitute for dependent care. During the time you are expected to work, you are expected not to be providing dependent care.

Taxes
It will be the employee's responsibility to determine any income tax implications of maintaining a home office area. RTHS will not provide tax guidance nor will RTHS assume any additional tax liabilities. Employees are encouraged to consult with a qualified tax professional to discuss income tax implications.

Communication
Employees must be available by phone, teleconference and email during core work hours.

Problem-Solving/Policies
RTHS understands that remote work may be challenging and RTHS will make every effort to support employees during this time. Employees are expected to assist in problem-solving any challenges they have while remote working and work with their supervisor and RTHS when such issues arise. Please keep in mind that employees remain obligated to comply with all School rules, practices, policies and instructions while telecommuting.

Attire/Conduct
Remote working employees are expected to continue to conduct themselves in a professional manner while working for RTHS. It is expected that remote working employees will be available for audio and video conferences/calls during working hours. Telecommuting employees must also be sure to dress professionally and appropriately as per School policy during work time, especially when conducting classes, meetings or communications using video.

Tracked Time Worked
Remote working employees who are not exempt from the overtime requirements of the Fair Labor Standards Act will be required to accurately record all hours worked using RTHS's time-keeping system. Hours worked in excess of those scheduled per day and per workweek require

the advance written approval of the Leadership. Failure to comply with this requirement may result in the immediate termination or termination of the remote working arrangement.

For exempt remote working employees, RTHS will set work expectations and accountability measures, which may differ based on position, grade level and subject matter. In addition, exempt employees may be required to track time and productivity.

Time off/Leave/Sick Time
All employees are expected to continue complying with RTHS's time off, leave and sick time policies. Reporting expectations under such policies shall continue to remain in effect with any modifications being communicated by your supervisor or RTHS's leadership.

Nothing in this policy shall be construed to alter any other term or condition of employment or any other RTHS policies, contracts or agreement.

Hardware

The Technology Department continues to adopt, review and update standards for the purchase of all hardware used at RTHS.

It is the intent to provide guidelines for a standard and controllable network environment in support of the mission of Research Triangle High School.

Hardware has been approved by the Director of IT based on the following criteria:

- Initial cost
- Impact on network and support
- Vendor economic strength, support, and expertise
- Product/technology maturity and availability
- Interoperability
- Use of industry-recommended design standards
- Documentation
- Security and internal control designs
- Learning curve and training requirement for end users
- Consistency with business and education strategies

Hardware Purchasing Standards
Limiting the number of different vendors and hardware types results in a lower initial cost as well as improved support by the technical support staff over time. The technology department will be knowledgeable of the product line and an inventory of appropriate repair parts can be maintained. Interoperability will be greatly improved.

Electronic Equipment - School Purchase
If a teacher or department is interested in purchasing any electronic equipment, they must first make the request with the IT department to evaluate for computer compatibility, network evaluation, etc. The proposal will then be reviewed by the Operations Director for approval.

Inventory
Any technology purchased, donated or crowd source funded must be inventoried by the technology department prior to delivery or use. Process of inventory will include description of the unit, date of purchase, price of the unit, department, and location. An asset label will be placed in a visible location that will allow the repair and check-in/check-out process to be more efficient.

The technology department will maintain a central inventory system of all inventory and will collect new data at the end of every year for auditing purposes.

Computer Repair
Research Triangle High School takes care of all of our own computer repairs and has a business agreement with Microsoft for rapid replacements. If your school issued computer is in need of repair, please email tech@rthighschool.org

Relocation of Equipment
The technology department should be contacted before any computer equipment is relocated. Depending on the situation, permission may be given for the staff to simply continue with the relocation of the equipment.

If the requested relocation requires technical assistance or reconfiguration of computers (such as moving computers to and from classrooms), you will be instructed to submit the request to tech@rthighschool.org

School-Based Programs Involving Technology
School-adopted program involving technology is the school's complete financial responsibility. This includes any hardware or software installed beyond the established computer standard provided by the technology department. It will be the school's responsibility for the purchase of the equipment, subscription fees and the logistics of the programs.

All computer equipment must be purchased according to the standards outlined in the Hardware section of this document. Any equipment types not listed there, such as cameras, wireless devices, etc. must be pre-approved before purchase. If approved, it will only be configured for the purpose of purchase, and not supported for personal or other use. For software to be run or used on these devices, please refer to the software section of this document.

Computer Donations
Research Triangle High School is happy to accept donated technology, however, in order to perform effectively within RTHS's network environment, donated computers must meet performance and license requirements.

Computers that do not meet hardware purchasing standards or do not meet the minimum standards for networking cannot be added to the RTHS network and will be donated to a local electronics recycler or Kramden Institute.

Donated equipment that meets hardware purchasing standards and meets the minimum standards for networking will be connected to the network. The tech department will provide ongoing support; however, it will not be included in the replacement schedule or be repaired.

Acquiring Technology by Grant or Crowd Sourced Funding
Any grant that is written must be approved by the Dean or Director of Operations and then the ED will review the grant based on the Internal Controls Policy. If the grant involves technology of any sort, it will also need approval of the Director of IT.

Any technology that is acquired through donations, grants or crowd source funding becomes the property of Research Triangle High School.

Employee-Owned Hardware
The Technology Department/Research Triangle High School does not support, nor is it responsible for loss, damage, movement, or theft of any non-school-owned hardware. This includes, but is not limited to computers, printers, cameras, laptops, etc.

In addition, the technology department will install or connect personal hardware to the network or printers. It reserves the right to remove any unauthorized hardware from the RTHS network.

In order to help maintain network security, any employee-owned hardware (cell phones, laptops, tablets etc.) that need to connect to RTHS's network must be authenticated via Meraki with their Google Workspace login credentials.

Checkout of Technology
Any equipment (document cameras, tablets, cameras etc.) that leaves school grounds must be checked out with the technology department before that property can be removed. Adhering to the RTHS Remote Working Policy, school owned technology can be checked out when working from home, as long as the Expectations for Technology Security are followed as outlined in the Remote Working Policy.

School purchased printers are prohibited from leaving RTHS's network without prior approval from the technology department.

School-Owned Hardware Use
As a courtesy, Research Triangle High School provides laptops to staff and faculty members and some students in order to meet their needs and fulfill their educational and occupational responsibilities. These laptops should not be used for personal gain, small businesses or illegal activities. Misuse of this technology will result in the laptop being taken away and a review by the Chief Operations Director.

Technology Life Cycle Replacement Plan

Introduction
This policy provides for scheduled replacement of computers for faculty, staff, and various classroom/campus technology every 36-48 months, dependent on funding. Eligibility for the equipment replacement is determined by the Information Technology staff in accordance with this policy which is reviewed annually by the Director of Operations.

Principle/Goals
The Technology Life Cycle Replacement Plan strives to provide the right tool to the students, staff, and faculty at the right time while using RTHS's limited resources efficiently in supporting the mission of the charter.
This can be accomplished by:

- Departments securing ongoing funds to replace technology and computer related equipment;
- Systematically and proactively replacing labs and employee computers on a three/four year cycle across the campus in a staggered manner vs one-at-a-time or all at once;
- Assuring that each faculty and staff member has computing resources of sufficient capability to fulfill his/her job responsibilities;

- Align with the RTHS Technology Standards, Policies & Procedures for minimum standards for communications, computing, network, and classroom equipment and promote uniformity of technology levels within RTHS;
- Providing for the cost effective and timely purchasing and installation of new equipment while decreasing the deployment time for new equipment;
- Expediting the disposal of old and obsolete equipment; and
- Replacing network printers, individual printers, scanners and peripherals on the same cycle as the computers.

Hardware Platforms

In order to contain costs and realize maintenance and support efficiencies, the RTHS community is provided with a list of approved computer systems from which to choose. The equipment standards are set according to RTHS Technology Standards, Policies & Procedures and guidelines.

Life Cycle Equipment Replacement Term

- Faculty/Staff Computers are replaced every three years (36 months), a duration that is a few months earlier than industry benchmarks.
- Classroom desktops are replaced every four years (48 months) funds permitting, a duration that corresponds to industry benchmarks for the useful life of laptop and desktop computer systems.
- Prior to the end of the 48-month term, those with a life cycle program asset in their possession will be contacted by the RTHS technology department, via email, to select a replacement computer and to establish a date for the equipment exchange.
- The Technology Life Cycle Replacement Plan provides an extended warranty on laptops for three/four years of the life of the equipment.
- All equipment (including cables, mouse, keyboard and other items delivered with the computer) must be returned to the technology department upon replacement.
- Replacement of computers is subject to available funding.
- Purchasing of laptop depends on funding and equipment availability and is subject to approval by Executive Director and is on case-by-case basis

Equipment Assignment

- As Personnel are hired, it is the responsibility of the Supervisor to ensure proper computing equipment and a phone are ordered and/or requested through college approved purchasing procedures.
- The Supervisor will coordinate with Human Resources to ensure account access is secured in a timely manner.

Responsibilities of RTHS Personnel Receiving Equipment

- RTHS Staff and Faculty are expected to exercise care to assure against theft and damage of equipment provided to them. In situations where negligence or violations of this policy result in damage or loss of equipment, the cost for its repair or replacement will be the responsibility of the employee. Physical negligence is determined by the IT department.
- Equipment is provided to RTHS personnel exclusively for their use. Its use by others is prohibited except for occasional use by other RTHS personnel. Equipment can be reallocated to another employee at RTHS but only with the proper documentation and must go through IT for refresh before changing hands.
- Upon separation from RTHS, for any reason, all equipment must be returned to the IT Department.
- All laptops and tablets must be brought to campus according to the audit procedures determined each year to receive software updates and for domain refresh.

- All equipment inventories will be the responsibility of the receiver and will not be moved without a movable property form.
- All laptop and portable devices must keep the "off campus use" form with the device when it leaves the campus.
- No user is granted Administrative rights to the assigned computer without the express permission of Chief Technology Officer.
- As equipment is replaced, old equipment will be relinquished to IT. A request may be made to the CTO for reallocation for another purpose but must be approved.

Default Equipment
The default computer platform for the Technology Life Cycle Replacement Program is a Microsoft Surface Laptop, Lenovo Desktop, and MacBook Air.

Exceptions to the Standard Build and Configurations
The specified equipment (the standard configurations), on occasion, may not meet the needs of a classroom, individual, or department. In such cases, alterations to the standard build configurations may be approved, but they must be authorized by the CTO and Director of Operations.

Exception Approval for Apple/Mac Devices and Rational for Deviation
There are provided specifications for Apple/Mac computing platform machines since there are individuals or operating units that require the Apple/Mac devices. Approval for the acquisition of an Apple/Mac device may be made by the CTO when there is a compelling demonstration of the need which cannot be met with the default PC. The approval process for Apple/Mac devices applies only to new requests for Apple/Mac equipment. Staff and faculty who already have an Apple/Mac device may replace it without obtaining special approval.

Retirement of Equipment
Once it has been determined the equipment will no longer support the mission of RTHS, it must be returned to IT for proper disposal. It is not acceptable for an employee to retain possession of equipment that is deemed unusable.

Software

In keeping with the content and philosophies of the *NC Standard Course of Study*, technology is placed in schools not only to support learning computer skills but also to provide activities that support and enhance the curriculum. Standardized age-appropriate software is selected that enables teachers at different grade levels to focus on specific areas of the curriculum or on different skills.

The technology department continues to review, update and adopt standard software for the school. All software must be approved for use by the technology department. This ensures a standardized and controllable network environment that supports the mission of Research Triangle High School.

Software is divided into two categories, standard software that is provided on all computers in a particular grade/area that may be purchased by schools or departments.

Standard Software
All RTHS network devices include a list of all standard software that is typically installed on every device. Different Operating Systems may require different versions of the software to be loaded and not all software is designed for all platforms. Therefore, a computer may not have everything on the list.

New software should be available in a current version that is designed to operate with Research Triangle High School hardware standards and installed operating systems. Beta and trial versions of software products cannot be considered. Approval by the technology department will be based on the following criteria:

- Initial cost
- Impact on network and support
- Product/technology maturity and availability
- Interoperability
- Use of industry-recommended design standards
- Documentation
- Security and internal control designs
- Learning curve and training requirement for end users
- Consistency with business and education strategies

Personally Owned Software
The Technology Department does not support any personally owned software. The technology department reserves the right to remove unauthorized software from the RTHS computer systems.

Employees should not download any personal software to their school issued devices unless approved by the technology department.

Network Access/Email

Network Access Policy
Research Triangle High School's data systems are provided as a central resource for RTHS staff and their students. It is important that the network infrastructure continues to develop with sufficient flexibility and security while at the same time remaining capable of exploiting anticipated developments in high-speed networking technology allowing expanded user services. As additional methods and approaches develop to access network resources, so must related access and management strategies to protect the network from unauthorized use.

Purpose
The purpose of a Network Access Policy is to establish rules for accessing and using RTHS network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of RTHS Confidential Information and Personally Identifiable Information (PII).

General
Authorized users are permitted access only to approved RTHS resources and systems. Users inside the RTHS firewall may not connect to the network if they are using a wireless connection to connect to an external network, an anonymizer, proxy, or VPN.

RTHS staff and users not involved directly in information security systems management shall not:

- Extend or re-transmit RTHS network services by installing a router, switch, hub, or wireless access point on any RTHS administered network
- Install any network hardware or software that provides network services without the express authorization of the Director of Operations or their designee
- Alter network hardware in any way

- Download, install, or run security programs or utilities that reveal weaknesses in the security of a system unless authorized by management
- Run password cracking programs, packet sniffers, network mapping tools, or port scanners

Management Responsibilities
The Director of Operations or their designee shall ensure procedures and controls exist that maintain and manage:

- Authorization and/or supervision of employees who work with sensitive information in locations where it might be accessed
- Approve IT to access information from the Google Workspace Vault
- Job descriptions that determine appropriate levels of access to sensitive information
- Access to sensitive electronic and paper information
- Employee access to sensitive information and the procedures are organizationally consistent
- Technical safeguards enabling the ability to manage sensitive information and protect against unauthorized access
- Access to sensitive information through a workstation, device, transaction, program, or process
- The manner in which sensitive job functions are performed and the physical attributes of devices that access sensitive information
- Identification and classification of devices that access sensitive information
- Workstation placement and position to only allow viewing by authorized individuals, including specification of additional security measures (e.g. privacy screens, password protected screen savers, auto logoff, etc.) to protect workstations with sensitive information
- Device use for users that access sensitive information from remote locations
- Application sessions termination after a specified period of inactivity
- Automatic logoff shall be implemented on all RTHS devices capable of this function
- Utility programs that might be capable of overriding system and application controls

Audit Controls and Management
On-demand documented procedures and evidence of practice should be in place for this operational policy as part of RTHS processes. Examples of suitable controls include:

- Regular and documented communications supporting execution of this policy
- Departmental procedures supporting policy
- Computerized logs where appropriate
- Implemented computerized group policy supporting access control and security
- Regular calendars supporting review, testing, and assessment of network access strategies

Security

The purpose of this policy is to ensure the secure use and handling of all RTHS data, computer systems and computer equipment by school students, patrons, and employees.

Technology Security

It is the policy of Research Triangle High School to support secure network systems in the school, including security for all personally identifiable information that is stored on paper or stored digitally on district-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the school, its students, or its employees. The school will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable. All persons who are granted access to the school network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of school devices and the network. When an employee or other user becomes aware of suspicious activity, they are to immediately contact the school's technology department with the relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to RTHS critically sensitive data. All third-party entities will be required to sign the Restriction on Use of Confidential Information Agreement before accessing our systems or receiving information. It is the policy of RTHS to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with local and state cybersecurity standards and regulations. RTHS supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect RTHS's data, users, and digital assets.

Procedure

Definitions:

- Access:
  Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.
- Authorization:
  Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.
- Computer:
  Any electronic device or communication facility that stores, retrieves, processes, or transmits data.
- Computer system:
  A set of related, connected or unconnected, devices, software, or other related computer equipment.
- Computer network:
  The interconnection of communication or telecommunication lines between: computers; or

computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

- Computer property:
  Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.
- Confidential:
  Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.
- Encryption or encrypted data:
  The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
- Personally Identifiable Information (PII):
  Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered protected data.
- Security system:
  A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.
- Sensitive data:
  Data that contains personally identifiable information.
- System level:
  Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Security Responsibility
RTHS Director of Operations or their designee are responsible for overseeing school-wide IT security, including and not limited to the development of school policies and adherence to the standards defined in this document.

Training
RTHS, led by the Chief Technology Officer, shall ensure that all school employees having access to sensitive information undergo annual IT cybersecurity training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all school employees.

RTHS, led by the CTO, shall ensure that all students are informed of Cyber Security Awareness.

Physical Security

Computer Security

- RTHS shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.
- RTHS shall ensure that all equipment that contains sensitive information will be secured to deter theft.
- RTHS shall ensure school managed devices hard drives are encrypted
- RTHS shall ensure that when laptops are reassigned or reallocated, hard drives are wiped using DoD Short - USA Department of Defense 5220.22-M short 3 pass wipe (passes 1, 2 & 7)

Server/Network Room Security

- RTHS shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.
- Telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to be opened.

Contractor access

- Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by RTHS's Technology Department.

Network Security

Network perimeter controls will be implemented to regulate traffic moving between trusted internal (school based) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

Network Segmentation

- RTHS shall ensure that all untrusted and public access computer networks are separated from main school computer networks and utilize security policies to ensure the integrity of those computer networks.
- RTHS will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

Wireless Networks

- No wireless access point shall be installed on RTHS's computer network that does not conform with current network standards as defined by the CTO.
- RTHS shall scan for and remove or disable any rogue wireless devices on a regular basis.

- All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

Remote Access
RTHS shall ensure that any remote access with connectivity to the school's internal network is achieved using the school's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the CTO.

Access Control
System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

Authentication
RTHS shall enforce strong password management for employees, students, and contractors and apply two-factor authentication when appropriate.

Password Creation
All server system-level passwords must conform to the Password Construction Guidelines posted on the Research Triangle High School.

Password Protection
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Authorization
RTHS shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

RTHS shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

Google Vault Authorization
Director of Operations expressly designates the technology department to be the sole users with access to the RTHS Google Workspace Vault.

Accounting

RTHS shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/configuration, and failed attempts to access objects by unauthorized users, etc.

Administrative Access Controls
RTHS shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

Incident Management
Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

Business Continuity
To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of school IT operations.

RTHS shall develop and deploy a school-wide continuity plan which should include as a minimum:

- Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- Secondary Locations: Identify a backup processing location, such as another School or District building.
- Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

Malicious Software
Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

- RTHS shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.
- RTHS shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
- RTHS shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.
- All computers must use the technology department approved anti-virus solution.

Any exceptions to section must be approved by the Director of Operations.

Internet Content Filtering
In accordance with Federal and State Law, RTHS shall filter internet traffic for content defined in law that is deemed harmful to minors.

RTHS acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, RTHS uses a combination of technological means and supervisory means to protect students from harmful online content.

In the event that students take devices home, RTHS will provide a technology based filtering solution for those devices to the extent practical and feasible . However, the school will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

Students shall be supervised when accessing the internet and using school owned devices on school property.

Data Privacy

RTHS considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

RTHS protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §62G-2 ("GRAMA"), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 ("COPPA").

RTHS shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

Security Audit and Remediation
RTHS shall perform routine security and privacy audits in congruence with the local and state cybersecurity guidance.

RTHS shall develop remediation plans to address identified lapses that conforms with the local and state cybersecurity guidance.

Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and District policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with RTHS.

Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

Establishing Network Access and Email Accounts for Employees
User accounts are automatically created for new employees of Research Triangle High School. Employees will be notified via email from IT of account information. Every employee should know his/her email user account name and password. Employees must be familiar with and adhere to the Acceptable Use Policy (AUP).

Each employee should keep his/her username and password secure and should not give it to anyone else for use. An employee's login information should not be given to students or non- employees to gain access to the RTHS network. All unauthorized access will be revoked.

The user's legal first initial and last name will be used to create network access and email accounts. Following a specific naming convention, the account uses first initial and last name ex. Jsmith@rthighschool.org

All questions concerning a user account should be directed to the technology department.

Name Changes for Network Access and Email Accounts
Network access and email accounts are based on the legal name of an employee. Name changes can be requested and approved by the Director of Operations.

Closing Accounts for Retirements, Resignations or Terminations
Email accounts will be suspended within 30 days of retirement or resignation of an employee. Terminations will result in immediate closing of email accounts.

Establishing Network Access and Email Accounts for Non-Employees
User accounts may also be provided to contractors and other companies, agencies or persons doing business with Research Triangle High School where Research Triangle High School benefits from the use of the account as determined by the technology department.

The department requesting network access or email accounts for non-employees should have all non-employees sign AUP forms and forward those forms to the Technology Department.

Requesting Password Reset
Staff/Faculty/Student Passwords: Requests for password resets (Google Workspace, PowerSchool, or school computer logins) can be made to tech@rthighschool.org

Security Policy
The Research Triangle High School network is "secured" by the following technologies including but not limited to Cisco Meraki, a cloud filtering service, network appliance based firewall. Google Workspace account information is used to log in and access the wireless network. Access varies according to the user identification and group.

All staff/faculty have a predetermined wireless network password set by the technology department that changes yearly and must also authenticate using their school managed Google Workspace account. They can download from the Internet and save data to their work devices. Personal devices must be approved for use by the technology department and meet security requirements.

Students use a predetermined password set by the technology department and must also authenticate using their school managed Google Workspace account. As a Bring Your Own Device school, students can download and save data to their personal devices as needed. Personal device use will be revoked if the student is found to be violating any policies while on the RTHS network.

Users should not modify policies, machine settings, or infrastructure to gain unauthorized access to resources or to circumvent established safety configurations. Any unauthorized changes or modifications made will result in loss of privileges and will be reviewed by the School Executive

Officer.

Filtering and Access to Information
The Internet provides access to material that may not be suitable for students and/or may not have educational value. In order to ensure that the internet connection is used in the appropriate manner and that all users are protected from any inappropriate information; the school has implemented a filtering system. All internet access is monitored for online safety and appropriate use. Zscaler filtering is used to filter internet traffic to block access to inappropriate sites as well as Cisco Meraki appliance based content filtering. Information is filtered by subject area and includes the filtering of visual depictions. The software has an override feature if filtered information is needed. Schools may also request that blocked sites be enabled through the technology department. The technology department will make the decision on 'relaxing' or 'enabling' a blocked site if it meets acceptable standards and is for bona fide research or other lawful purposes.

Personal Use of Email
Email accounts are provided to all employees and students and should be utilized for school-related purposes and performance of job duties. Incidental personal use of email is permitted as long as such use does not interfere with the employee's job duties, the performance of system operations or other email users. Incidental personal use is defined as use by an individual employee for occasional personal communications. Such personal use must comply with the Acceptable Use Policy and other applicable policies of the school. Employees are reminded that there is no expectation of privacy provided.

Management of Email Accounts
The email system is provided for the purpose of communication, not as a storage device. Individual users must assist in the management of this valuable resource.

Mass Distribution of Email
Employees are limited to distribution of email to their site only. Email should not be used for any type of personal gain including, but not limited to, money-making schemes, advertising and sales. The distribution of mass emails and chain letters is prohibited.

Release of Email Addresses
The release, publication or distribution of Research Triangle High School email addresses to any outside party whose intent is to communicate with email account holders is prohibited. An email address may only be given to an outside party by the owner of that email address.

Confidential Information and Use of Email
The Family Educational Rights to Privacy Act (FERPA) and RTHS Policies address the issues associated with the confidentiality of student and employee records. Use of email as a means of communications is subject to all current laws and RTHS policies and must be used with due regard for the need to maintain confidentiality.

Other confidential information that would jeopardize the operations of Research Triangle High School may not be released to anyone outside the system. Information such as passwords, security information, data network information, etc. would be considered confidential.

Privacy of Email/Calendars
Email and calendars are not private. Research Triangle High School is the owner of all information sent using the school's email and calendar system. Employees are reminded that there is no expectation of privacy provided. Emails and calendars are public record. All email correspondence

and calendar information is subject to the North Carolina Records Law, which may result in monitoring and disclosure to third parties. All communication should be conducted with this in mind. Employees and students should not use the school calendars for personal events or link personal calendars to the school calendar. RTHS will not be responsible for incidental use or disclosure of personal information released resulting from improper use of RTHS's calendar system.

Although Research Triangle High School does not make a practice of monitoring these messages, Research Triangle High School reserves the right to access email at any time for troubleshooting, security, and maintenance purposes as well as any situation in which life, limb or property is in perceived danger. Other access to email including, but not limited to, criminal investigations, civil investigations and supervisory investigations may be approved by the Executive Director or Board of Directors.

Users should be aware that during the performance of their duties, the technology department personnel need from time to time to observe certain functions of the email system and on these occasions may inadvertently see the contents of email messages. Except as provided elsewhere in this policy, they are not permitted to see or read the contents intentionally or to read transactional information where not germane to the foregoing purpose or to disclose or otherwise use what they have seen unless there is reason to believe that laws or RTHS policies have been violated.

The technology department may need to inspect mail that has been deemed "undeliverable", is suspected of virus content and for other troubleshooting purposes.

Surveillance Camera Policy

Research Triangle High School seeks to promote and foster school safety and a safe and effective educational and work environment. After having carefully considered and balanced the individual's right to be free from invasion of privacy with the School's interest and duty to promote the health, welfare and safety of students and staff as well as the health, safety and welfare of members of the general public who have occasion to use school facilities and enhance the protection of school property, the School supports and reserves the right to place and use surveillance cameras, when necessary and appropriate, in the school, school facilities, school buses and/or on its school grounds.

Purpose of Surveillance Cameras

The primary uses of surveillance cameras are as follows: (i) to promote a safe environment by deterring conduct that violates the law, School Committee policy and/or school based rules; and (ii) to record images for future identification of individuals in the event of violations of law, School Committee policy and/or school-based rules; (iii) to aid in search of lost or missing children, and (iv) to assist emergency services personnel. Surveillance camera use is limited to uses that do not violate federal or state constitutional protections against unreasonable search and seizure, reasonable expectation of privacy and other applicable laws prohibiting wiretapping and electronic surveillance of aural communications. Surveillance cameras will be utilized in public areas of schools, school facilities, school buses and school grounds and in areas of schools, school facilities, school buses and school grounds deemed to be at risk for either vandalism or student misconduct. Surveillance cameras will not be used in the private areas of restrooms, showers, locker rooms and dressing rooms and any other area in which there is a reasonable expectation of privacy. Surveillance cameras also will not be used in private offices and classrooms. The use of surveillance cameras and the monitoring of any resultant recordings will be conducted in a professional, ethical and legal manner and in a manner consistent with all

existing Research Triangle High School policies and state and federal laws and will not be based on a subject's personal characteristics, including race, gender, ethnicity, sexual orientation, disability or other protected characteristics.

Monitoring

School employees involved in video monitoring of public areas will perform their duties in accordance with the practices outlined in this policy.

Video surveillance monitors shall be located in areas to which access is controlled and shall not be viewable by unauthorized persons.

Video recording may only be monitored by the Executive Director or Director of Operations. No unapproved employees may monitor or view video or camera images for any reason except as necessary in the course of an investigation or adjudication.

Any employee violating this policy may be disciplined, up to and including termination. Information obtained in violation of this policy shall not be used in any disciplinary proceeding against a Cambridge Public Schools' student and/or employee.

All staff approved to monitor video or camera images shall receive a copy of this policy and provide written acknowledgment that they have read and understand this policy.

A log will be maintained by the Director of Operations that will record the name and date anytime a staff member other than Director of Operations views a recording.

Storage

Any video recording used for surveillance purposes in schools, school facilities, school buses and/or on school grounds shall be the sole property of Research Triangle High School and stored for no more than one month after which such recordings will be promptly erased unless retained as part of a criminal investigation, court proceeding (criminal or civil), or other bona fide use, as approved by the Executive Director or designee; and the Executive Director or designee will be the custodian of such recordings and all such recordings shall be properly protected from unauthorized viewing. A record log will be kept of all instances of access to and use of recorded material.

Release of Information

Requests for viewing a recording must be made in writing to the Executive Director or designee and all public records requests for recordings that are received will be forwarded to the Legal Counsel for review. The request shall identify the individual for whom access is sought, the date(s) and/or time period(s) for which access is sought, and the rationale why access should be granted. If the request is granted, such viewing must occur in the presence of the Executive Director or designee. Under no circumstances will the School video recording be duplicated and/or removed from the School premises without the express written authorization of the Executive Director of Schools or designee.

Destruction and/or Tampering with Surveillance Cameras

Any individual who tampers with or destroys a video surveillance camera or any part of the video surveillance system will be subject to appropriate disciplinary action as well as possible criminal charges.

APPENDIX A

Expectations for Technology Security
Working remotely has its benefits but doing so comes with the added responsibility of taking the appropriate steps to protect your organization's data while being connected online. Keep these tips in mind.

- **Know RTHS's remote work policies**
  This includes when and where it is acceptable to work away from the office as well as any security measures or best practices.
- **Use only devices approved by your organization**
  Avoid using personal computers, tablets and cellphones - as well as those shared with others - to work.
- **Use VPN when necessary**
  Virtual private networks, which provide secure direct connections to your organization's computer network, might be necessary when accessing files, working with sensitive information or using certain websites.
- **Think before you click**
  Avoid downloading or clicking on unknown links in emails. If you aren't sure if you should, call the sender first. Hackers often use fake websites to trick you into giving sensitive information or to install malware onto your device.
- **Guard your devices**
  If your organization allows you to work elsewhere from your home, never leave your laptop, tablet or cellphone - including any USB or external storage devices - unattended. Avoid entering passwords where others can see.
- **Connect only to trusted networks or your cellular Wi-Fi connection**
  Public hotspots aren't secure and might not protect your passwords, emails and potentially sensitive work.
- **Create strong passwords**
  Be sure they include a mix of upper and lowercase letters, numbers and symbols. Make them difficult enough that someone can't guess them.
- **Don't share passwords online**
  If you must share log-in information with a coworker, call them with the details instead of sending via email, text, or instant message.
- **Use two-factor authentication**
  Although it can be inconvenient, two-factor authentication, if available, provides an extra layer of security to keep hackers from accessing accounts.
- **Encrypt your email**
  Some data and information might need to be encrypted before sending electronically. This might also include information that you might otherwise share in a conversation if you were at the office,
- **Contact your IT help desk**
  If you need technical support, contact RTHS's IT department. Don't try to fix technical issues yourself.

APPENDIX B

Acceptable Use of Technology
Research Triangle High School recognizes that technology and the Internet offer students and staff the resources of thousands of computers all over the world and to millions of individual people. Students, teachers, and staff may have access to: 1) electronic mail (e-mail) communication with people all over the world; 2) information and news, some of which may include advertisements, from a variety of sources and research institutions; 3) discussion groups on a wide variety of topics; 4) access to many university libraries, the Library of Congress and other libraries around the world.

Research Triangle High School Network and internet connection have been established in the belief that the information and interaction made available are valuable additions to educational resources.

The intent of this policy is to ensure that all uses of Research Triangle High School technology and the internet are consistent with the goals and educational philosophy of the school system.

Basic tenets of the policy are:

- The use of technology resources and internet access is to support research and education and to extend the resources of Research Triangle High School.
- All use of technology must be in support of education, research or enrichment and be consistent with the intended purposes.
- Technology Department is responsible for establishing **and users are required to follow all** standards, policies, and procedures related to the use of technology in the Research Triangle High School.
- Use of other organization's networks or computing resources must comply with the rules appropriate for that network.
- Transmission of any material in violation of any law or system policy is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, material protected by trade secret, material used for commercial activities by for-profit institutions, and material used for product advertisement or political lobbying.
- Students, teachers and staff members will be informed of issues regarding network etiquette, security and vandalism with the understanding that any violation of the regulations is unethical and may constitute a criminal offense or violation of the "Student Code of Conduct," and require appropriate disciplinary action.
- Research Triangle High School does not endorse or authorize the use of any of its school names in any electronic medium, examples are websites, user groups, uniform resource locators (URL's), unless express written consent is granted by the Research Triangle High School.

Network Etiquette
The use of technology requires that you abide by accepted rules of etiquette which include, but are not limited to, the following:

A. Courtesy: Do not send or forward abusive messages to anyone.
B. Appropriate Content: Defamatory, intentionally inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing or illegal material is prohibited.
C. Privacy: All communication and information accessible via the network should be assumed to be copyrighted property. Transmission of data on the Internet cannot be guaranteed to be private or secure. Note that electronic mail (email) is not guaranteed to be private. People

who operate the system do have access to all mail and electronic transmissions. Electronic transmissions relating to or in support of illegal activities may be reported to the authorities. Do not reveal your or any individual's personal address, phone or credit card number.

Email
Limited personal use of email is permitted; however, personal use should not interfere with assigned duties and responsibilities. The use of email requires that you abide by accepted rules of etiquette which include, but are not limited to, the following:

A. SPAM, the sending of unwanted mail is a significant problem for users and for the network. Do not send emails that are not directly business or school related to groups or persons within the system.
B. Using RTHS email directories or address books to send emails that are for personal gain or that promise personal gain are a violation of Administrative Policy.
C. Use of RTHS email directories or address books to communicate views, solicit membership, or raise funds for any non-school sponsored purpose, whether profit or non-profit, is prohibited
D. The technology department will distribute virus warnings. If you feel you have information regarding a virus, please contact network administration immediately and do not forward such emails to users.
E. **Email is not private**. **Access is usually limited to investigative or troubleshooting purposes, however, the Executive Director may at any time, and for any reason, allow the search of email or data stored on all school owned computers.**

Passwords
Passwords are personal and should not be shared with anyone. Attempts to login to the system as any other user will result in cancellation of user privileges and/or criminal prosecution. RTHS will follow NCDPI password requirements to ensure the security of student data.

Copyright
Information transmitted through the Internet which is copyrighted is subject to the same copyright laws as govern non-electronic data.

Security
Security on any computer system is high priority, especially when the system involves many users. If you feel you can identify a security problem on the service provided you, notify a system administrator or teacher. Do not demonstrate the problem to other users.

Plagiarism
Data received through the Internet is subject to the same rules of documentation as traditional information. Give credit for all material used in research.

Vandalism
Vandalism will result in cancellation of your privileges. This includes, but is not limited to altering web sites, intentionally damaging equipment or cabling, uploading or creation of a computer virus, and any other activity that corrupts individual programs, data or the network.

Network resources
The user is responsible for his or her actions and activities involving the network. Some examples of

unacceptable uses are: wastefully using resources such as file space, circumventing safety configurations, modifying setup policies, modifying settings on machines, attaching unauthorized devices, modifying infrastructure, invading the privacy of individuals, gaining unauthorized access to resources or entities, using the network while access privileges are suspended or revoked.

Emerging Technologies
The tenets of the AUP are inclusive of emerging technologies in devices that provide wireless capabilities. Examples of these devices include but are not limited to, IoT devices, "smart" glasses, etc. The following are not permitted uses of these devices by students on Research Triangle High School campuses and school related activities:

- Connecting to unfiltered Internet information.
- Using such a device to capture images, transmit, and manipulate media electronically.

One example of an inappropriate use is using a camera phone to take pictures, emailing the pictures, then posting these pictures on the web. Student use of these devices is not allowed without written permission from Research Triangle High School administrative staff with expressed intent and purpose for use.

Teachers and staff members that have devices capable of these functions are guided by the tenets of the AUP are to ensure that no privacy rights are violated regarding Family Education Rights Privacy Act (FERPA).

The use of technology resources and Internet access is a privilege and not a right; inappropriate use will result in cancellation of those privileges. Do not use the network in any way that will disrupt the use of the network by others. Technology Department may make decisions regarding whether or not a user has violated standards, policies or procedures; and may deny, revoke, or suspend access at any time.

School Issued Technology
RTHS technology is inventoried by the school system software and checked out to staff members. Once technology is checked out to employees or student, it becomes their responsibility. Each year, employees will sign the AUP with the understanding that if an employee is terminated voluntary or involuntary, all equipment will be returned to the Director of Operations. If any equipment is damaged through negligence or lost, RTHS will deduct the cost of the item(s) from the employee's final paycheck, except where deductions are prohibited by state law.

Upon my termination from Research Triangle High School, either voluntary or involuntary, I will return all of the item(s) listed above to the Director of Operations. If any items are missing or have been damaged through my negligence, I authorize Research Triangle High School to deduct the cost of the item(s), as indicated above, from my final paycheck, except where deductions are prohibited by state law.

Web 2.0/Social Networking Tools:
Web 2.0/Social Networking Tools are a catch all phrase used to describe technology which integrates technology, social interaction and content creation.

Limited use of Web 2.0/Social Networking Tools are permitted; however, personal use should not interfere with assigned duties and responsibilities.

Some examples are:

- Blogs

- Chat Rooms
- Podcasts
- Social Networking (Twitter, Instagram, Facebook, etc)
- Virtual Spaces

Employees should familiarize themselves with RTHS Code of Conduct found in the Employee Handbook and other guidelines/resources (such as the Social Media Guidelines) posted on the Research Triangle High School web site that provide direction for employees participating in online social media activities.

The use of Web 2.0/Social Networking Tools requires that you abide by acceptable rules of etiquette.

The following conducts are discouraged:

- Engaging in vulgar or abusive language, personal attacks, or offensive terms targeting individual and/or groups
- Endorsement of commercial products, services, or entities
- Endorsement of political parties, candidates, or groups
- Lobbying members of any elected body using resources of RTHS.

Issues to be aware of:

- Items published on the web are persistent. You should consider all items published on the web to be public domain.
- When discussing item(s) involving RTHS or RTHS related matters you may wish to contact the Executive Director prior to publishing content.
- Per the State of North Carolina guidelines for school system employees, you must maintain an appropriate relationship with students in all settings.
- Access to social media must be closely monitored to ensure that it is appropriate for student use. The educator is solely responsible for the content they allow students to view.
- When posting to web sites outside of RTHS you may wish to include a disclaimer such as, "The postings on this site are my own and do not necessarily reflect the views of Research Triangle High School."
- Do not reference your position within the RTHS system when writing in a nonofficial capacity.
- Respect copyright laws.
- Make sure your online presence reflects how you wish to be seen by the public as a RTHS Professional.
- Have no expectation of privacy.

Internet Safety and Children's Internet Protection Act (CIPA) and Research Triangle High School Student Email Accounts

The Children's Internet Protection Act ("CIPA"), enacted December 21, 2000, require recipients (Research Triangle High School) of federal technology funds to comply with certain Internet filtering and policy requirements.

Access to Inappropriate Material

To the extent practical and feasible, technology
protection measures (or "Internet filters") are used to block or filter Internet traffic, and other forms of electronic communications (student email). Access to inappropriate information as required by the Children's Internet Protection Act, will be filtered or blocked this is applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Inappropriate Network Usage

To the extent practical and feasible technology and policies are used be to promote the safety and security of users of the online computer networks when using electronic mail, other forms of direct electronic communications inappropriate network usage includes, but is not limited to:

A. unauthorized access, including so-called 'hacking,' and other unlawful activities;
B. unauthorized disclosure, use, and dissemination of personal identification information regarding students.
C. using another student's username and password to access network resources
D. transmitting obscene or pornographic visual imagery, harassing, menacing or any type of language that is deemed profane, cyberbullying, threatening; any communication that indicates fear or intimation to an individual or groups of individuals.

Education, Supervision and Monitoring

While RTHS takes considerable steps to electronically block inappropriate materials and sites, it is the responsibility of all school staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet.

- Students, teachers and staff members will be informed of the intent of the Acceptable Use Policy by its inclusion in the Student Handbook and Employee Handbook.
- The school will provide teachers, students and parents with guidelines and various computerized informational resources for the protection of students while using technology. The resources will be age-appropriate and designed to promote student safety with regard to Internet usage. This includes lessons on cyberbullying, appropriate online interactions and the use of social networking sites.
- Cyberbullying is the act of bullying or harassment through the use of any electronic means. Any form of cyberbullying is strictly prohibited and will result in appropriate disciplinary action. Students should promptly disclose to their teacher or other school official any inappropriate, threatening, or unwelcomed message.
- Technology Department for Research Triangle High School will supervise and monitor usage of school resources, the network infrastructure, and access to the Internet in accordance with this Policy and the Children's Internet Protection Act. Any use of an electronic medium connected to these resources (an example is, but not limited to; student email accounts) is governed by this Policy.
- Anyone found violating tenets of the AUP, the Children's Internet Protection Act (CIPA) or Research Triangle High School Student Email Accounts provision will have their access revoked and will be subject to the actions defined in the Student Code of Conduct.
- Procedures for the disabling or otherwise modifying of any technology protection measures shall be the responsibility of Research Triangle High School Technology Department or designated representatives.

APPENDIX C

Troubleshooting
Suggestions to keep your computer equipment running correctly:

When possible, before trying anything else, attempt to **REBOOT** your computer. Save any work, close all programs, shutting down and powering off your device can resolve many problems.

- Check for pending Windows updates and install every other week
- Do not cover the cooling vents on the computer.
- Keep the computer area free from the buildup of dust.
- Do not eat or drink close to the computer.

Nothing seems to be working	✓ If it's a desktop, make sure the computer is plugged in and powered on. If it's a laptop, make sure the battery is charged, plugged in and powered on. ✓ Check for secure cable connections on back of computer for keyboard, mouse, etc
Cannot reach desired web site on Internet	✓ Check the web address for accuracy ✓ Try to connect to a different site. ✓ Try to connect to the desired site from another computer or ask a colleague; also try a different browser or incognito window
Computer Frozen	✓ Press **CTRL, ALT, DEL** buttons simultaneously ✓ Choose **Select Task List** ✓ Highlight programs shown as **Not Responding** ✓ Press **End Task** button ✓ **Be patient**; this may unfreeze computer ✓ If possible, shut computer down properly ✓ **If fails to unfreeze**, only option is to power off