SERIES 500

TECHNOLOGY

POLICIES AND PROCEDURES

Approved by Board on August 7, 2023

Two Rivers Community Charter School

Table of Contents

500 TECHNOLOGY – POLICIES AND PROCEDURES

501 GENERAL PROVISIONS

501.1 Scope and Purpose

These policies shall govern the use of the School's technology resources and, to the extent allowed by law, the use of personal technology resources as they impact the School. Technology resources will be used as a resource for fostering academic and operational excellence.

501.2 User Risk

Officials of the School will strive to take all reasonable measures to minimize the risks associated with technology use. Nevertheless, users must exercise reasonable care to avoid such risks for themselves.

501.3 Limitations

The availability to users of the school's technology resources, particularly of electronic communications tools like e-mail and the Internet, is intended primarily for furthering the school's educational mission and not for any non-educational personal user benefit.

501.4 Ownership, Monitoring, and Control / No Expectation of Privacy

All school technology resources are owned or leased by the School. Use of the school's technology resources is a privilege, not a right. The School reserves the right to direct, monitor, control, and limit or revoke the use of those resources. The availability of these resources does not confer upon any user a legal expectation of privacy, free from such monitoring or control.

501.5 Reporting Misuse or External Threats

Any member of the school community should promptly report any violation or threat of violation under these policies to an appropriate school official.

502 ALL SCHOOL TECHNOLOGY USERS

502.1 Overview

This policy regarding acceptable and prohibited uses of technology resources applies to all users of the School's technology resources: students, employees, board members, contractors, guests, and other authorized individuals. It shall be enforced in conjunction with all other technology resources and general policies.

502.2 Permissible Uses

The School's technology resources are employed to fulfill the purposes directly related to its educational mission and programs, and in support of users' roles within the School. Unless otherwise prohibited, personal or incidental use of school technology resources is permitted if such use conforms to these policies, is reasonably limited, and does not interfere or threaten to

interfere with school's operation.

502.3 Prohibited Uses

Users of school technology resources shall not intentionally or negligently engage in any of the following.

502.3.1 Unlawful or Generally Prohibited Uses

Users may not use technology resources in violation of any local, state, or federal law, or any other school policy or rule.

502.3.2 Harassing, Intimidating, Bullying, and Other Similarly Offensive Uses

Users may not use technology resources to engage in conduct involving harassment, intimidation, bullying, discrimination, or similarly offensive or harmful communications as defined and prohibited by any other school policies. This includes conduct that:

a. a reasonable person should know, under the circumstances, will have the effect of harming or humiliating a student or damaging the student's property or of placing a student in reasonable fear of harm to their person or damage to their property; or

b. has the effect of insulting or demeaning any student or group of students in such a way as to cause substantial disruption in, or substantial interference with, the orderly operation of the school.

502.3.3 Disrupting or Damaging Uses

Users may not use school technology resources in any way that threatens their safe, secure, and orderly operation. This includes, but is not limited to, creating, installing, or forwarding computer viruses; consuming inordinate and unauthorized electronic storage space; sending "chain letters," "spam" e-mail, or similar types of communications; or downloading software, media files, or data streams without proper authorization.

502.3.4 Unauthorized Technology Access, Endangerment, or Tampering

Users may not obtain, alter, obstruct access to, or in any other way intrude upon or damage the School's or any other user's computer files, programs, or hardware without proper authorization.

502.3.5 Jeopardizing or Bypassing School Security Measures

Users shall not, without proper authorization, intentionally disclose or aid in the disclosure of computer passwords, codes, or similar information designed to secure the school's computer resources and to protect private or confidential information. Users also shall not intentionally bypass Internet filters or other devices or measures used by the School to restrict access to school, the Internet, or other electronic information. In addition, users shall not provide information or other means to allow others users to engage in similar bypassing activity. Thus,

for example, using or providing information about Internet proxy sites to bypass school internet filters is prohibited.

502.3.6 Promotional Uses and Advocacy

Users shall not use the school technology resources for commercial gain or for political, social, religious, or other personal advocacy except as allowed by right under law and otherwise permitted.

502.3.7 Publishing Personal Information on the Internet

No user shall electronically distribute or post personal information about themself or about any other person associated with the School unless (a) the distribution is legal and properly authorized by school officials, and (b) the distribution does not or is not likely to threaten that person's or any other person's privacy or safety.

502.3.8 Downloading or Copying Files or Data

Users, without proper authorization and legal right, may not download programs, files, or other data onto school computers or other technology equipment. This includes downloading or copying entertainment audio or video files and images, software, or other similar data not directly related to school objectives.

502.3.9 Unauthorized Users

Users of school technology resources may not permit, without proper authorization, any person to use such resources who is not a member of the school community or not otherwise authorized to have such access. Users are prohibited from using another individual's computer account or accessing such person's electronic data without prior permission from an authorized official.

502.3.10 Plagiarism and Related Acts of Academic Dishonesty

Users shall not use technology resources to plagiarize or otherwise illegally copy or use another person's work or to engage in any other form of academic dishonesty.

502.3.11 Copyright and Software Copying

Users shall not use school technology resources in violation of state or federal copyright laws. Users shall not, without proper authorization, copy school-owned computer files or software onto any computer. Use of any files, software, or other program or data must be authorized and legally licensed or permitted for such use.

502.3.12 Off-Campus and Personal Technology Use

The School reserves the right, to the maximum extent permitted by law, to discipline or take any other action against persons related to their personal electronic technology use (e.g., communications generated via private computers and/or Internet accounts) when such use poses a substantial threat to others' safety or to the operations of the School. This includes uses that

cause or are likely to cause a substantial disruption or material interference with the school's educational objectives or operations, or that otherwise injure or threaten to injure persons or property within the school community.

502.3.13 Representation of the School's Viewpoints and Positions

Views and position statements may be expressed as representing the position of the Board, administration, or staff only with prior approval by the Director (or designee). Otherwise, no user may use any technology resources to communicate in a way that indicates or implies that the views or positions expressed are established, supported, or endorsed by the Board, its administrators, or other school officials.

502.3.14 Violating the School's Trademark, Copyright, and Other Intellectual Property Rights

Users may not copy, mimic, sell, or otherwise use the school's trademarks, images, documents, or other intellectual property without proper and legal authorization. The School reserves all rights to such intellectual property.

503 STUDENT USE

503.1 Overview

This policy establishes proper and improper student uses of technology resources in conjunction with other related policies. Students users must be familiar with and comply with this policy, the General Provisions (Policy 501), General Use Policy for All Users (Policy 502), and any other applicable policies and rules.

503.2 Enforcement

School officials retain reasonable discretion to apply this and related school policies to determine when a proper or improper use exists and what sanctions, if any, may apply.

503.3 School and Parental Responsibilities

The School and its staff seek to take all reasonable measures to guide, monitor, and protect students in their use of the school's technology resources, consistent with student age and maturity. Parents, however, are primarily responsible for instructing their children in the proper values governing the use of such resources. The School requests that parents, in cooperation with the School, communicate to their children an understanding of responsible and safe use of these resources and to monitor their children's use of such resources at home or anywhere outside the school's jurisdiction.

503.4 Permissible Uses

School technology resources are to be used for educational, organizational, and communication purposes directly related to the school's educational mission and program. Unless otherwise prohibited, limited personal or incidental use of school technology resources is permitted if such

use complies with these policies, is reasonably limited, and does not interfere or threaten to interfere with the school's operational and educational objectives.

503.5 Prohibited Uses

Students shall not engage in prohibited uses of technology resources. Prohibited uses include, but are not necessarily limited to, the following types.

503.5.1 General Prohibited Uses

General prohibited uses include all uses prohibited in the School's General Use Policy (Policy 502).

503.5.2 Social Networking Sites

A student may not use social networking sites on campus unless such use is explicitly authorized by an appropriate school official, is used for school-related instructional purposes, and such use is consistent with school and individual school policies. In addition, a student may not use technology resources, including the Internet and e-mail, to arrange for him/herself or any other student to meet another person. Social Networking sites include, but are not limited to Internet sites like MySpace or Facebook, Blogs and other Internet sites involving publication or interaction of a personal nature.

503.5.3 Disclosing Personal Identifying Information

In addition to related prohibitions in the General Use Policy (Policy 502) students are prohibited, without proper authorization, from disclosing personal identifying information about themselves or others through the use of the School's or personal technology resources while on school premises or during school functions. "Personal identifying information" includes, but is not necessarily limited to, a person's name, phone number, address, e-mail address, social security number, or other information that is reasonably likely to allow a person's identity to be determined from disclosing such information outside the school community.

503.5.4 Off-Campus and Personal Technology Use

The School reserves the right, to the maximum extent permitted by law, to discipline a student for off-campus or other personal electronic technology use (e.g., communications generated via private computers and/or Internet accounts). This includes uses that cause or are likely to cause a substantial disruption or material interference with the school's educational objectives or operations, or that otherwise injure or threaten to injure persons or property within the school community. In addition, violators may also be subject to civil or criminal actions and penalties under local, state, and federal laws.

503.5.5 Personal Electronic Devices

Except as permitted by this policy or other school rule or directive no student shall, during regular school hours or while participating in school-sponsored curricular functions, turn on or

use a personal electronic device, except in urgent or emergency circumstances. Any device used in violation of this policy may be confiscated by the Director (or designee) consistent with other school policies and rules. Similarly, the Director (or designee) may determine the terms under which the device may be returned to the student or student's guardian. Notwithstanding the prohibited uses identified above, exceptions to such prohibited uses shall apply in the following circumstances:

a. when the Director (or designee) permits a student or students, in case-by-case instances, to turn on or use such electronic device(s) if there is a reasonable need to do so, or

b. emergency conditions exist which seriously threaten one's safety or property, and such use is the only reasonable means of avoiding such threat, or

c. when the Director (or designee) determines that such use, generally, is otherwise necessary or prudent and is not in violation of any other law or policy. Personal electronic devices may be used after regular school hours and at extra-curricular school functions when such use is:

   i. consistent with other student conduct policies;

   ii. does not or is not likely to disrupt any school function or operation; and

   iii. has not otherwise been prohibited by the Director or their designee.

504 EMPLOYEE USE

504.1 Overview

The School provides employees with technology resources to support the school's educational, organizational, and communication objectives. Like any other educational resources, employees are expected to exercise sound judgment when using technology resources in their professional roles. This policy establishes proper and improper employee uses of these resources in conjunction with other related policies. Specifically, employees shall comply with this policy, the General Provisions (Policy 501), General Use Policy for All Users (Policy 502) and any other applicable policies. An "employee," for purposes of this policy, is anyone retained to carry out the work of the School including, but not necessarily limited to, paid employees, board of education members, contractors, consultants, temporary staff members, and volunteers.

504.2 Enforcement

School supervisory officials retain reasonable discretion to apply this and related school policies to determine when a proper or improper use exists and what sanctions, if any, shall apply.

504.3 Employee Role in Promoting Safe and Effective Student Use

All employees are expected to model and promote proper technology use for and by students. Employees should take all reasonable measures, consistent with their job duties, to guide,

instruct, monitor, and protect students in their use of the school's technology resources.

504.4 Permissible Uses

The school's technology resources are to be used for educational, organizational, and communication purposes directly related to the school's mission and objectives. Unless otherwise prohibited, personal incidental use of school technology resources is permitted if such use is consistent with these policies, is reasonably limited, and does not interfere or threaten to interfere with the school's operations or with the performance of an employee's duties. Supervisors retain discretion to curtail or prohibit personal use of technology resources by any subordinate employee or student.

504.5 Ownership, Public Records, and Record Retention

Employees shall use technology resources subject to the following principles and requirements set forth elsewhere, including Policy 506 (Operational Use Policy).

504.5.1 Right to Control, Monitor, and Search All Electronic Files

The School owns and has the right to control, monitor, and search technology resources issued to employees as well as any data, files, or other product of such use, to the maximum extent allowed by law.

504.5.2 Electronic Files as Public Records

All records generated by employees in their use of the school's technology resources are or may be public records to the extent that such records relate to the conduct of the business of the School. Such records include, but are not limited to, any electronic document such as a memo, letter, spreadsheet, financial compilation, or database; e-mail messages; and Internet usage records (e.g., cookies, Internet logs, data downloads). Therefore, the School may be required to make such records available for public inspection unless such records are otherwise protected from disclosure by law.

504.5.3 Electronic Public Records Subject to Record Retention Rules

Any electronic file or data that is a public record is subject to federal, state, and local record retention rules. All employees will be instructed in and shall comply with such rules, including those rules contained in other Technology Policies.

504.5.4 Personal Electronic Data

Personal files, data and other electronic information ("personal electronic data") generated or stored on technology resources or networks owned or issued by the School is subject to control and inspection by appropriate school officials even though such personal electronic data is not a public record. Employees who generate such personal electronic data, consistent with reasonable personal use rules, shall delete or remove such data from the school's technology resources and networks within a reasonable time. Such deletion and removal must take place immediately if the

presence of such data interferes with or is likely to interfere with the safe, efficient, and orderly operations of the School.

504.6 Prohibited Uses

An employee shall not engage in prohibited uses of technology resources. Prohibited uses include, but are not necessarily limited to, the following:

a. General Prohibited Uses

Prohibited uses include all prohibited uses contained in the School's General Use Policy for All Users (Policy 501) and other applicable policies.

b. Improper Destruction of Public Records

Any electronic record that pertains to the conduct of business of the School is a public record and may not be destroyed or altered in any way unless permitted by law and local rules and procedures.

c. Improper Disclosure of Confidential Information

Employees shall not disclose to unauthorized recipients any electronic file or other information that is protected from such disclosure by law or local policy. This includes but is not limited to protected personnel files, student records, or other organizational data that is exempt from public records rules.

d. Unauthorized Websites and Other Electronic Postings

Employees shall not, without proper authorization, send or post webpages, e-mail messages, blogs, or other electronic communications that bear the name of, represent, or otherwise imply the sponsorship or activity of the School. This prohibition includes, but is not limited to, school, class or club related webpages, blog sites, listserv communications, social networking, or other website postings and communications.

e. Improper Instructional Uses

Instructional staff and supervisors shall not engage in instructional uses of technology resources that are contrary to policies and rules governing such uses under Policy 505.

f. Personal Technology Resources to Conduct School Business

Unless otherwise authorized or approved by proper supervisory staff, employees shall not use personal electronic devices to create, store, transmit or otherwise process electronic data and communications when such use involves any of the following:

i. private, confidential, or otherwise sensitive educational or school school-related information;

ii. school public records when such information is not also contained in appropriate computer or other electronic media owned or controlled by the

School; or iii. school information when such use otherwise impedes or is intended to impede the ability of the School from complying with all public records, record retention, open meetings, and related laws and rules. Examples of such prohibited conduct include, but are not limited to:

(i). Using a personal computer, laptop, or other similar device to view or store confidential student, employee, or other school-related records;

(ii). Using a personal digital camera or cell phone to create, store, or transmit pictures, records, or other information that is otherwise protected from public disclosure;

(iii). Using personal e-mail to conduct school business; or iv. Posting or storing protected school or job-related information on a private, non-school website or other technology venue.

504.7 Potential Sanctions and Liability

An employee who violates any of these policies may be subject to disciplinary or other legal actions initiated by the School, other government agencies, and/or by aggrieved persons or entities. Such actions may include, but are not limited to, one or more of the following:

a. Warning or reprimand;

b. Curtailment, suspension, or revocation of technology resource privileges;

c. Suspension with or without pay;

d. Demotion or loss of salary;

e. Termination of employment;

f. Licensure sanctions;

g. Personal civil liability and damages for conduct within and/or outside the scope of the employee's duties; or

h. Conviction for a criminal offense.

505 INSTRUCTIONAL

505.1 Overview

Like any means of instruction – textbooks, worksheets, blackboards, etc. - technology is an aid to learning, albeit a remarkable and growing one. It is, however, the ends, objectives, and measures of education, not their means that ultimately determine instructional effectiveness. For this reason, the use of technology as a means of academic achievement should always be measured by how well it facilitates the ends – i.e., the fundamental objectives – of education: student learning, critical thinking, and character development. As long as technology offers the best

means to foster these educational objectives, the School seeks to promote its safe, legal, and responsible use. Technological advances in society undeniably require the use of technology in education. The availability of new technological tools challenges educators to consider their use to enhance student instruction. The School recognizes the need to seize the useful opportunities these tools offer. Balancing efficiency and student safety with educational quality and innovation, the School encourages the use of these tools in a way that promotes its mission and academic objectives and is safe, legal, and age- and pedagogically-appropriate.

505.2 General Considerations

505.2.1 Instructional Technology Use and Resources

Instructional technology use (ITU) generally refers to the use of traditional and emerging electronic devices and other means of communication available for teaching.

505.2.2 Technology Proficiency

Federal and State Law, including the North Carolina Standard Course of Study, mandate that students be proficient in the use of technology. Teachers and administrators, increasingly, should model such proficiency. Recognizing that the abilities of individual staff members to integrate technology into classroom instruction vary widely; all instructional staff are nevertheless expected to increase their technological proficiency whenever it will reasonably improve their instructional effectiveness.

505.2.3 Legal Considerations

Instructional staff shall be informed of and, to the extent feasible, trained in sound legal and pedagogical ITU. Predominant legal considerations include:

a. First Amendment:

   i. Preserving, except where appropriate, all school-related websites and other electronic forums as “closed forums” and, therefore, not expanding the First Amendment rights of students or other users when using such forums unless otherwise interested and approved.

   ii. Understanding that the use of technology resources does not convey or involve any constitutional right of academic freedom for instructional staff;

   iii. Refraining from limiting student use of otherwise available technology in a way that infringes their free speech rights, either to express or to access information or ideas.

b. Privacy and Confidentiality: ITU must avoid the disclosure of sensitive, personal, or confidential information in violation of state or federal records and sound ethical considerations.

c. Defamation and Harassment: ITU must not include communications that allow or foster harassing, defamatory, intimidating or other harmful or potentially harmful expression.

d. Copyright and Trademark: ITU must avoid the unauthorized use of protected intellectual property without permission or by legal right to do so.

e. Public Records and Retention: ITU must not involve the illegal production or destruction of electronic records or files that constitute public records and/or that must be stored or archived under state or federal record-keeping requirements.

f. Local Policies and Procedures: ITU must conform to all other objectives, policies, rules, and practices of the School and its constituent schools. This includes following all procedures for review and approval of instructional technology resources.

505.2.4 Limitations and Caveats

Instructional staff should always be mindful of the limitations and dangers of technology. For example, much information on the Internet is of questionable validity or accuracy. Therefore, a more traditional means of obtaining information or teaching a particular subject may be required. Because the School cannot guarantee the educational value of information accessed electronically, instructional staff is expected to use sound judgment and discretion when planning for ITU.

505.3 Acceptable Instructional Technology Uses and Guidelines

505.3.1 General Acceptable Use

School technology resources are to be used for educational, organizational, and communication purposes directly related to the School's educational mission and program. ITU should always be consistent with principles of effective pedagogy and with all other policies pertaining to proper instruction and technology use. Furthermore, instructional staff shall make reasonable efforts to supervise a student's use of the Internet and other electronic resources during school-sponsored activities

505.3.2 Guidelines for Determining Acceptable ITU

The following criteria should guide the consideration and implementation of ITU:

a. Educationally Important and Appropriate

Any ITU in question should be the most or one of the most effective ways of instructing students on a particular matter. It should also account for the age, maturity, and skill levels of student users. If another means of instruction exists that is more effective, it should normally be selected except for other compelling reasons. Technology should not be used as end in itself; e.g., just because others are using it or because it is readily available or easy to use.

b. Administratively Manageable

ITU should not require an undue consumption of resources (e.g., finances, time, supervision) compared to other traditional means of instruction. Generally, ITU should save time or offer better educational value compared to traditional instruction except when the ITU offers other compelling benefits. Instructional staff should be sufficiently skilled to implement the ITU effectively.

c. Operationally Compatible

ITU should not interfere with, obstruct, or otherwise be incompatible with the network, hardware, or software used by the School. Instructional staff should confer and, where necessary, obtain approval for ITU if there is a risk or uncertainty regarding the compatibility of a particular ITU.

d. Legally Permissible

Instructional staff should be adequately informed of the legal principles applicable to ITU. Instructional staff should ensure that their ITU is legally permissible by confirming its propriety with and obtaining approval from appropriate supervisory staff or legal counsel in accordance with applicable procedural requirements. If uncertainty exists as to the legality of any ITU, instructional staff shall refrain from such use until proper approval is granted.

e. Locally and Logically Consistent

ITU shall conform to all other school policies, rules, and practices and with general principles of sound pedagogy and prudent judgment.

f. Publicly Defensible

Instructional staff should consider how any ITU would be viewed in the public eye, especially by the parental community. If reasonable doubt exists as to public perceptions of the ITU, instructional staff shall seek advanced approval from an appropriate supervisor and, when appropriate, from the parents of the students who would experience the ITU.

505.3.3 Creation and Publication of School-Related Webpages and Web Content

Web pages produced, maintained, and/or supervised by instructional staff must conform to any Webpage Development standards and rules approved by the Director (or designee). Unless otherwise provided, instructional staff members responsible for a school webpage are also responsible for editing and controlling its content. Such editorial control remains subject to review by the Director (or designee).

505.3.4 Electronic Publication of Student-Authored Materials

Students may not post a webpage within, or linked from, another school webpage unless the student webpage is for instructional or other school-related purposes. Such student pages shall be

subject to instructional staff supervision and control and, to the extent the page reveals information about the student or any other person associated with the School, requires advanced approval from the Director (or designee).

505.4 Prohibited Uses

505.4.1 Generally Prohibited Uses

General prohibited uses include those identified in the School Policy 502 and other technology policies.

505.4.2 Unauthorized Use of Personal Technology Resources

Unless otherwise approved by an authorized school official, ITU shall not involve personally-owned electronic communication forums and devices or those owned, created, or operated for personal use. This includes, but is not limited to, the use of personal websites, e-mail addresses or networks, blogs, social networking sites, PDAs, or any other communication forum or technology device. Furthermore, school webpages shall not include links to student or employee personal webpages or other electronic communication forum without advanced approval by appropriate supervisory personnel and assurances that such use furthers an important educational purpose without creating a foreseeable risk of harm or liability.

505.4.3 Non-Approved Uses

Instructional staff shall avoid any ITU that has not received proper advanced review and approval by supervisory staff or other authorized individuals. The School may establish additional procedures for specific types of ITU in line with school policy. In cases when uncertainty or ambiguity exists as to whether advanced approval is required for a particular ITU, instructional staff shall seek approval from appropriate supervisory staff for such use

505.4.4 Unauthorized Opening of Free Speech Forums

Students do not shed their free speech rights when they are at school. However, their rights are limited because, under First Amendment Law, public schools are a “closed forum” with a defined purpose of educating students. Therefore, in ordinary circumstances, school officials may reasonably regulate and direct curricular matters and classroom activities (i.e., take actions that are “reasonably related” to any “legitimate” school purpose). A school's “closed forum” might become an “open forum” and subject to greater First Amendment scrutiny if school officials or employees do anything that invites students, parents, or other members of the public to express their viewpoints beyond the narrower boundaries of instructional assignments. For instance, a teacher who creates a website for posting student opinions, but does not carefully define the purpose of the site and the rules for expression, might, in that instance, inadvertently “open” or “broaden” the speech forum. The effect of this action could render comments made on the site protected speech. This could be the case even if objectionable or offensive to some readers. Thus, instructional staff shall not, without prior supervisory consideration and approval,

prepare and implement ITUs such as a class blog site, listserv, chat room, or webpage that invites student expression beyond specific curricular boundaries. If permission for such a site is granted, the instructor shall clearly communicate to students or other users the limited educational or school-related purpose of such forum along with specific instructions and guidelines for conforming to that purpose. No school electronic forum shall be "opened" or "widened" under the First Amendment without good reason and without careful supervisory deliberation and approval and, where necessary, the advice of legal counsel. Specifically, ITU shall be limited to strictly school-related purposes consistent with the educational objectives and policies of the School. In all cases where reasonably feasible, ITU shall include a clear notice to students and other authorized users of the specific purposes, guidelines, and rules for engaging in the ITU.

505.4.5 Copyright Violations

The School prohibits copyright violations. Instructional staff members are expected to exercise diligent care to ensure their use of ITU and that of their students does not violate this prohibition. The use of others' materials is appropriate and, in fact, encouraged to accomplish legitimate instructional objectives when such use is properly approved by the property holder, is exempted by the copyright doctrine of fair use, is part of the public domain, or is permitted by other legal means. Instructional staff should, in advance, consult appropriate supervisors and resources to determine how their planned ITU complies with copyright rules and exceptions. The School and its Director shall strive to ensure that instructional staff are regularly notified and adequately informed of copyright principles and/or available resources in relation to ITU.

505.4.6 Safety and Confidentiality Threats

Instructional staff shall not engage in ITU that creates an undue risk of disclosure of confidential or sensitive student or other personal information, including but not limited to, disclosing student identifying information such as student names, contact information, grades, or pictures, unless a disclosure involves "directory information" or is otherwise properly approved.

505.4.7 Harmful, Disruptive, or Threatening Off-Duty or Personal Uses

Instructional staff shall not, whether on or off duty, engage in personal communications or other electronic activities (e.g., the use of personal websites or other non-school pages or forums, personal social networking sites, personal blog sites, personal e-mail) when such use causes or is likely to cause harm, substantial disruption, or material interference related to any individual, operation, or property of the School.

505.5 Procedures

505.5.1 Notification, Awareness, and Training

Instructional staff members are expected to be familiar and to comply with these and other policies and procedures related to ITU. The Directors or their designees shall strive to regularly inform and educate instructional staff regarding such policies and procedures.

505.5.2 Review and Approval of ITU

The Director or their designee may develop rules and guidelines for reviewing, recommending, and approving ITU those recommended by the Technology Director or other technology staff.

505.5.3 Waivers and Exceptions

Any instructional staff member may request a waiver or exception to any provision within this Instructional Use Policy pursuant to any employee grievance or other applicable procedure. Any request for a waiver or exception and any decision in response thereto, shall normally be documented in writing and a copy provided to the Director (or designee).

506 OPERATIONAL USE

506.1 Overview

The backbone of effective technology use involves commitments, policies, and practices to support safe, efficient, and beneficial implementation. The School is committed to providing a sound operational infrastructure through this and related technology policies. This policy shall be interpreted and applied consistently with other technology policies of the School.

506.2 School Control and Personal Computers

All computers and other technology resources owned by the School are under the control of the School, including hardware, software, and data and word processing files stored on such computer and related equipment. No personal software, media files or other large data files, are to be kept on the computers without prior approval. Approved personal software or files are not to be used on the computer unless sufficient steps, as defined by the Executive Director or their designee, have been taken to protect a computer from viruses or any other potential damage.

506.3 Planning, Coordination, and Policy Development

The Director, with assistance from other staff or panels, shall periodically audit, assess, and strategically plan for effective technology use in the School. Such assessment and planning should occur frequently enough to allow for necessary modifications in policy and practice that reflect changes in technical, instructional, and legal developments.

506.4 Information Management

The School shall strive to implement and maintain an efficient and orderly system of recording, maintaining, protecting, and disposing of electronic records to conform with effective organizational practices and legal requirements, particularly regarding privacy and confidentiality, accessibility for necessary administrative and legal disclosure, public access, and record retention and disposal. An “Electronic Record” is defined as a record created or reproduced in any medium by means of any system requiring the aid of electronic technology to make the record readable or otherwise comprehensible by ordinary human sensory capabilities.

The state Department of Cultural Resources (DCR) offers guidelines and practices to guide state

agencies.[1] The Director and technology staff shall strive to remain informed of best practices and legal requirements in order to continually monitor and improve the school electronic data management practices. School officials responsible for record management and disposal should participate in training available to them for such purposes. All school staff should also be trained in proper electronic records management.

506.4.1 Network Monitoring and Privacy

The School shall implement all reasonable measures necessary to protect sensitive and confidential school records from unauthorized or accidental access, manipulation, and disclosure. Technology users who are responsible for preserving the integrity of school records should be trained regularly regarding the measures they are to employ. Examples of common confidentiality violations to be protected against include:

a. mistaken network or website availability or network hacking of personal information such as social security numbers, passwords, student grades, or personnel data;

b. posting student identifying information on school webpages;

c. sending confidential information via e-mail to improper recipients; and

d. leaving confidential information open on computer screens or other equipment and available for unauthorized viewing; improperly downloading, storing, or sharing confidential information on personal computers or devices.

506.4.2 Public Records Compliance

North Carolina's public records law establishes the public's right of access to all government records except those specifically exempted. Public records include, all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. Particular electronic requirements apply as follows:

a. Database Indexes: requires schools to maintain an index identifying the contents of all databases.

b. Accessible and Reliable Data Storage: requires a determination that an agency network or computer system will not impair the public's right to inspect the records maintained in that system.

c. Inspection Format: entitles members of the public to receive requested documents "in any and all media in which the agency is capable of providing them,"

[1] https://archives.ncdcr.gov/government (Apr. 28, 2023).

including electronic files. (This does not require, however, an agency to put into an electronic medium any document not kept in such format.) Examples of electronic records conveyed or stored on School equipment that may be subject to public records laws and production requests include: e-mail messages involving the conduct of school business, internet usage data (including cache files, websites histories, "cookies," downloaded documents), and phone and text message records. Staff of the School should always be mindful to use school technology resources as public stewards of such resources and strive to use them in a way that, if publicly disclosed, would reflect well on the staff and the School. The Director, with the assistance of the Technology Director, public records employees, and other staff, shall ensure that electronic public record files are preserved, accessible, and made available for public inspection and preservation according to state guidelines.

506.4.3 Indexing of Computer Databases

All computer databases compiled must be indexed as required by law. The form and content of the indexes will conform to the guidelines issued by the North Carolina Division of Archives and History. Any computer database that is being considered for purchase or lease by the School and that will be subject to the indexing requirements should include the statutorily required index provided by the vendor at no additional cost to the School.

506.4.4 Record Retention

State law and effective management practices require certain electronic records to be stored and preserved for varying lengths of time depending on their value. State law states that

> "Public record" or "public records" shall mean all documents, papers, letters, maps, books, **photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records**, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions."[2]

And, additionally

> "No public official may destroy, sell, loan, or otherwise dispose of any public record, except in accordance with G.S. 121-5 and G.S. 130A-99, without the consent of the

[2] G.S. 132.1(a) https://www.ncleg.gov/EnactedLegislation/Statutes/HTML/BySection/Chapter_132/GS_132-1.html (Apr. 28, 2023).

Department of Natural and Cultural Resources…. "[3]

Thus, to the extent that electronic records fall into the same categories as their hardcopy counterparts, they are subject to the same general retention requirements unless otherwise directed.

The School, unless otherwise approved by the Board, shall maintain its public records (electronic or otherwise) in accordance with the DCR Record Retention Schedule for Local Public School Units.[4]

506.5 Procurement, Maintenance, and Disposal of Technology Resources

The School shall strive to procure, maintain, and dispose of technology resources and materials in a legal and cost-effective manner, consistent with the School's mission. 506.5.1 Guidelines for Procurement

Technology resources are to be purchased and used which best promote the school's educational mission and comply with its policies and governing laws, including state bidding and purchase requirements. Procurement decisions should be guided by prudence, including but not limited to, the following principles and practices:

a. The resource is necessary to support, directly or indirectly, the educational and/or operational objectives of the School.

b. The resource is compatible, or can be made compatible, with other technology resources, including the School network.

c. The Technology Director will set minimum standards for technology resources that are purchased or donated. Upgrading, hardware conditions, and similar requirements will reflect high performance standards.

d. Staff training should be offered where necessary to maximize the benefits of technology resources.

e. Sufficient staff and other support exist to adequately evaluate, use and maintain technology resources.

The Technology Director and staff shall develop procedures for the maintenance, upgrading,

[3] G.S.132.3(a) https://www.ncleg.gov/EnactedLegislation/Statutes/HTML/BySection/Chapter_132/GS_132-3.html (Apr. 28, 2023).

[4]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiyiK-g2bj9AhXwlmoFHQfTDyMQFnoECAgQAQ&url=https%3A%2F%2Farchives.ncdcr.gov%2Fmedia%2F810%2Fopen&usg=AOvVaw1TTck_yEICqpM3Ma5YAgsu (Apr 28, 2023).

replacement, and disposal of technology resources. This shall include provision for donations to and from the School. These procedures shall follow state rules and guidelines and prevailing best practices.

506.6 Security

The Director, with the assistance of the Technology Director and staff, shall develop and implement reasonable measures to secure School technology resources and data from damage, theft, unintended disclosure, and other measures that threaten technology resource integrity and user safety and rights.

506.6.1 Passwords and Access

All technology users of the School shall normally be required to identify themselves by using a user identification (ID) and personal password before using the School network or any other major technology resources, such as workstations and computers. The Technology Director and staff shall implement and oversee the assignment of user IDs and passwords and other processes to protect against unauthorized user access, damage, and harm. Users who no longer are a part of the School community or otherwise not entitled to use its technology resources shall have their access rights terminated or limited promptly.

506.6.2 Vendor and Other Outside User Access

Vendors, consultants, or contractors retained by the School and volunteers, government agents, or other individuals not a regular part of the School community may require access to technology resources and to school data, some of which may be confidential including access codes, user records, or other sensitive information. The Director, with the aid of the Technology Director and other staff or committees, shall implement any procedures and rules necessary to minimize the risk of a breach to network and technology security, privacy, or integrity, using as necessary, prevailing practice standards, protocols, and rules. All staff involved in hiring and oversight for such outside users shall be regularly and fully informed of these protocols and rules and trained in their implementation and in security protection.

506.7 E-Copyright

Electronic documents can be reproduced and distributed electronically with great speed, ease, and anonymity. This significantly increases the potential for liability of the School and its agents. Users may not illegally copy another person's copyrighted materials, including those available or obtained via electronic sources such as e-mail or the Internet unless (1) the material is in the public domain, (2) the author grants permission to do so, or (3) the use is permitted by some exception in the copyright law, the most common and widely applied being the "fair use" exception to the federal Copyright Act. The fair use exception applies in contexts such as teaching, scholarship, or research and involves consideration of four primary factors: (a) purpose and character of the use; (b) nature of the copyrighted work; (c) amount and substantiality of the

portion used in relation to the work as a whole; and (d) effect of the use on the potential market for the copyrighted work.

507 BOARD USE

507.1 Overview

The use of technology resources by members of the Board, due to their unique status and role, is subject to certain special considerations and requirements addressed in this policy. Board members shall comply with these requirements and shall report to the board chairman or to the entire board, as the case may require, any abuses thereof by any board member or employee.

507.2 Permissible Uses

Board members may use school technology resources to fulfill their responsibilities in furtherance of the school's educational mission. Board members shall engage in such use in a responsible and prudent manner. Unless otherwise prohibited, limited personal or incidental use of school technology resources is permitted if such use complies with school policies, is reasonably limited and not disruptive, and does not interfere or threaten to interfere with the operational and educational objectives of the School or violate any law.

507.3 Prohibited Uses

Board members shall not engage in any prohibited uses of technology resources. Prohibited uses include, but are not necessarily limited to, the following uses.

507.3.1 General Prohibited Uses

General prohibited uses include all uses prohibited in the School General Use Policy (Policy 502).

507.3.2 Personal Use and Gain

Technology resources shall not be used for inordinate personal use or for personal advancement. Board members shall not allow any other person to use any technology resource, including a school-owned laptop computer issued to the board member, unless such other use is by a school official and necessary for the board member to carry out their duties.

507.3.3 Circumvention of Public Records, Confidentiality, or Open Meetings Laws

Technology resources may not be used to communicate or create records that violate the state's public records and open meetings laws. Board members shall not access or disclose to unauthorized recipients any electronic file or other information that is protected from such access or disclosure by law, local policy, or generally accepted ethical principles. This includes but is not limited to protected personnel files, student records, or other organizational data that is exempt from public records rules.

507.3.4 Use of Personal Technology Resources to Conduct School Business

Unless otherwise authorized or approved, board members shall not use personal electronic devices to create, store, transmit, or otherwise process electronic data and communications when such use involves any of the following:

a. Private, confidential, or otherwise sensitive school-related information;

b. School public records when such information is not also contained in or conveyed to appropriate computer or other electronic media owned or controlled by the School;

c. School information when such use otherwise impedes or is intended to impede the ability of the School from complying with all public records, record retention, open meetings, and related laws and rules; or

d. Circumvention, intentional or otherwise, of state or federal law. Examples of such prohibited conduct include, but are not limited to:

    i. Using a personal computer, laptop, or other similar device to view or store confidential student, employee, or other school-related records unless otherwise authorized;

    ii. Using a personal digital camera or cell phone to create, store, or transmit pictures, records, or other information that is otherwise protected from public disclosure;

    iii. Using personal e-mail to conduct school business unless such use is otherwise authorized or necessary; or

    iv. Posting or storing protected school or job-related information on a private, non-school website or other technology venue unless otherwise authorized.

507.4 Open Meetings

In North Carolina the public is entitled by law to observe the official meetings of public bodies like school boards, subject to certain exceptions. The state's open meetings law defines an official meeting as any "meeting, assembly, or gathering together at any time or place or the simultaneous communication by conference telephone or other electronic means of a majority of the members of a public body" to conduct its business. The law requires a public body to provide advance notice when it will conduct business through electronic means and must "provide a location and means" by which members of the public may "listen" to the meeting. Although this provision was written primarily with telephone conference meetings in mind, it also applies to e-mail, "chat rooms," "blogs," and other electronic forums as well. Thus, when a majority of board members communicate via e-mail or other electronic means about school business, the

communications are presumably subject to the Open Meetings law, at least to the extent that the communications are deemed to occur "simultaneously." Board members should be aware of these requirements and should not use e-mail or other electronic devices to circumvent the Open Meetings law.

507.5 Public Records and Record Retention

All records generated by board members in their use of school technology resources are or may be public records to the extent that such records relate to the conduct of the business of the School. Such records include, but are not limited to, any electronic document such as a memo, letter, spreadsheet, financial compilation, or database; e-mail messages; and Internet usage records (e.g., cookies, Internet logs, data downloads). Therefore, the School may be required to make such records available for public inspection unless such records are otherwise protected from disclosure by law or subject to disposal by approved record disposal schedules. For these reasons, any such records must be created, retained, and stored according to the school record retention policies. They may not be deleted or discarded except as permitted by the School's record retention policy. Typically, e-mail that has lost its value may be discarded; however, board members should be cautious to avoid premature or otherwise improper storage and deletion of such records to avoid subjecting themselves and the School to potential liability. Personal files, data and other similar electronic information (i.e., "personal electronic data") generated or stored on technology resources or networks owned or issued by the School should be kept to a minimum. Such data, though it is not a public record, may be subject to control, monitoring, and inspection by appropriate school officials. Board members who generate such personal electronic data, consistent with reasonable personal use rules, should delete or remove such data from school technology resources and networks within a reasonable time. Such deletion and removal must take place immediately if the presence of such data interferes with or is likely to interfere with safe, efficient, and orderly operations of the School.

507.6 Waivers and Exceptions

Board members may request waivers and exceptions to this policy by submitting such request to the whole Board.