Technology Policy
and
Acceptable Use Agreement

RIVERMONT COLLEGIATE0
1821 Sunset Drive
Bettendorf, IA 52722

563-359-1366 | 563-359-7576 | RIVERMONTCOLLEGIATE.ORG

Updated September 2020

Contents

Technology Policy

Purpose

The Rivermont Collegiate Board supports the use of the Internet and other computer networks in the School's instructional and operational programs to facilitate learning, teaching, and daily operations through interpersonal communications and access to information, research, and collaboration. It is the intent of Rivermont Collegiate to promote responsible, ethical, and appropriate use of information technology and network resources.

With Internet and e-mail access comes the availability of material that may not be considered appropriate in a school setting. The School cannot regulate and monitor all the information received or sent by persons who use the Internet or e-mail; and the School cannot ensure that students who use the network, Internet, or e-mail will be prevented from accessing inappropriate materials or sending or receiving objectionable communications. The School believes, however, that the availability and value of the Internet and e-mail far outweigh the possibility that users may procure inappropriate or offensive materials. Access to the school information technology and network resources is a privilege, not a right. Staff and students will be held accountable for noncompliance with this policy.

Authority

The School reserves the right to log, monitor, and review Internet, e-mail, and other network use of each user. This logging, monitoring, and review may be conducted without cause and without notice. Each user of a school computer or the school network, by the use thereof, agrees and consents to such logging, monitoring, and review and acknowledges that s/he has no right or expectation of confidentiality or privacy with respect to Internet, e-mail, or other network resources. Users should expect that files stored on school servers or computers will not be private.

The School employs the use of an Internet filter as a technology protection measure pursuant to the Children's Internet Protection Act. The filter may not be disabled or bypassed by students or other minors for any reason.

All students, administrators, and staff members who use the Internet, e-mail, and other network facilities must agree to and abide by all conditions of the policy. The School makes no warranties of any kind, whether express or implied, for the service it is providing.

The School is not responsible, and will not be responsible for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruption. Use of any information obtained through the use of the school network is at the user's risk. The School disclaims responsibility for the accuracy or quality of information obtained through the Internet or e-mail.

The School assumes no responsibility or liability for any charges incurred by a user. Under normal operating procedures, there will be no cost incurred.

A user may not install any software onto school devices and/or network drivers or disks unless s/he has the specific, prior written permission from the technology department.

Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Data Definition and Ownership

Rivermont Collegiate defines data as any information about individuals or intended for individuals within the Rivermont community. Data can take any form, including but not limited to paper records, electronic records, web materials, e-mails, PDF and other image files, streamed video, recorded video, etc.

All data generated by Rivermont and its employees, physical and/or electronic, is the property of Rivermont Collegiate. Any unauthorized access, retention, or distribution of data owned by Rivermont may result in disciplinary and/or legal action.

Users have the responsibility to respect and protect the rights of every other user in the School and on the Internet. The administration shall have the authority to determine what is inappropriate use.

Students and Staff are provided 1 Terabyte of storage space through a Microsoft Office 365 account to store/backup/save files. Students and Staff are also encouraged to back up all files to a flash drive or other online or external storage system.

Delegation of Responsibility

The Headmaster or designee shall be responsible for implementing technology and procedures to determine whether the School's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the administration.
2. Maintaining and securing a usage log.
3. Monitoring online activities.
4. Providing training to minors in appropriate online behavior. This includes behavior when interacting with other individuals on social networking websites, and in chat rooms, and cyberbullying awareness and response.

Guidelines

Procedures

Network accounts or access to the Internet will be used only by the authorized user for its authorized purpose. Network users shall respect the privacy of other users on the system. Account/Access will be granted to only those individuals who meet the following requirements:

1. Students must have read the Internet Access Agreement Form and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate school authority. Students must have their parent/guardian sign the signature page indicating the parent's/guardian's acceptance of the policy and agreement of the terms of the policy and their consent to allow the student to access and use the network.
2. Students and employees must have received instruction on network access, use, acceptable versus unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities.

General Prohibitions

The use of the Internet computer network for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. The administration reserves the right to determine if any activity constitutes an acceptable or unacceptable use of the network. With respect to all users, the following are expressly prohibited:

1. Use in an illegal manner or to facilitate illegal activity.
2. Use for commercial, private advertisement, or for-profit purposes.
3. Use for lobbying or political purposes.
4. Use to infiltrate or interfere with a computer system and/or damage to data, files, operations, software, or hardware components of a computer or system.
5. Hate mail, harassment, discriminatory remarks, threatening statements and other antisocial communications on the network.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Use to access, view or obtain material that is obscene, pornographic, including child pornography, or harmful to minors.
8. Transmission of material likely to be offensive or objectionable to recipients as determined by school administration.
9. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
10. Impersonation of another user, anonymity, and pseudonyms.
11. Loading or using of unauthorized software or media.
12. Disruption or distraction of the work of other users.
13. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
14. Quoting personal communications in a public forum without the original author's prior consent.
15. Use of the name of the School and use of written logos or web content provided by the School through its web site without the written permission of the Headmaster.
16. Allowing an unauthorized person to use an assigned account.
17. Creation and introduction of computer viruses, trojans, worms, and other malicious programs.
18. Use of software or hardware to compromise or bypass network security.
19. Bullying/Cyberbullying.
20. Use while access privileges are suspended or revoked.
21. Any attempt to circumvent or disable the filter or any security measure.
22. Use inconsistent with network etiquette and other generally accepted etiquette.

Student Prohibitions

1. Disclose, use, or disseminate any personal identification information of themselves or other students.
2. Engage in or access chat rooms or instant messaging without the permission and supervision of a teacher or administrator.

Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

1. Be polite. Do not become abusive in messages to others. General school rules and Board policies for behavior and communicating apply.
2. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
3. Do not reveal personal information, such as addresses or telephone numbers of others.
4. Recognize that e-mail is not private or confidential.

5. Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other users.
6. Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital status, or handicap status.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or School files. Each user is required to report any security problems to the Technology Director. The problem is not to be demonstrated to other users. To protect the integrity of the system, the following guidelines shall be followed:

1. Users shall not reveal their passwords to another individual.
2. Users are not to use a computer or network resource that has been logged in under another User's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences of Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate, willful, or negligent acts.

Illegal use of the network: intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

The use of the Internet and network resources is a privilege, not a right. School administrative staff, along with the Technology Director, will deem what is appropriate and inappropriate use and their decision is final.

Loss of access and other disciplinary actions shall be consequences for inappropriate use. Consequences of violations may include:

1. Suspension of information network access.
2. Revocation of information network access.
3. Suspension of network privileges.
4. Revocation of network privileges.
5. Suspension of computer access.
6. Revocation of computer access.
7. School suspension.
8. School expulsion.
9. Report of violation of local, state or federal laws to appropriate legal authorities.
10. Dismissal from employment.
11. Legal action and prosecution by the authorities.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to:

1. Creating or spreading computer viruses, worms, trojans, and other malicious programs.
2. Compromising network security.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc. All school computers/servers utilized by students and staff shall be equipped with Internet blocking/filtering software.

Internet safety measures shall effectively address the following:

1. Control of access to inappropriate matter on the Internet and World Wide Web.
2. Safety and security when using electronic communications.
3. Prevention of unauthorized online access including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information.
5. Restriction of minors' access to materials harmful to them.

Technology Policy During Distance Learning

Parent Support During Distance Learning

Parents play an important role in helping students succeed, particularly during distance learning. While support needs vary across the developmental spectrum, Rivermont recognizes that distance learning places additional responsibilities on parents. Even older students will need additional support while distance learning, so it is essential that parents become proactive in communicating with their children, teachers, and the school administration. The following is a partial list of recommended areas of parent support:

- Teach independence by helping your student think through how they might solve problems on their own. This will vary by developmental ability, but Rivermont's goal is to have teachers supporting students as they learn to tackle challenges themselves.
- Set up a specific learning space (if possible) that is separate from areas where the student relaxes when not working. Having an area designated and reserved for academic work will help students switch their thought modes and focus on academic work.
- Be sure that you have provided the necessary technological equipment and services that your child will need while distance learning. This includes internet, printer, webcam, microphone, and a suitable computer. See the technology section of our Back to School plan for more information.
- Help students organize their materials, file organization systems (both paper and electronic). Even older students who claim to not need organization support often benefit from talking through their system with a parent.
- Discuss assignment tracking with your child and know where they (and you) can look to see what they have turned in and what remains incomplete or not submitted. If the student doesn't know, help them think through how to solve that challenge, rather than solve it yourself (if possible).
- When in doubt, ask. Teachers and administrators are caring and committed to students' success but we cannot anticipate every challenge.

- Establish consistent routines that are comparable to those when at school. Sleeping and waking cycles, meal times, study sessions, and study breaks should be thought out in advance.
- Begin and maintain an open dialogue about stress and mental wellness during distance learning. Encourage exercise and perspective-building activities, such as mindfulness, meditation, yoga, etc.

Intended Digital Classroom Experience and Limitations

There is no substitute for the quality of interacting with a teacher and peers face-to-face. Distance learning in real-time streaming online classes is a distant second, in terms of teaching effectiveness and learning outcomes. Technology performance, internet speeds, and other logistical challenges are a natural and expected part of the online learning experience. Watching a recorded class video after the fact is even less effective than participating in real-time distance learning. For this reason, Rivermont encourages families to attend in person whenever safely possible, as determined by Rivermont, local health officials, and parents.

It is not Rivermont's goal to recreate the in-class experience for online students. Teachers have been given a directive that they should focus primarily on students attending face-to-face. While teachers are expected to engage online students, our goal is that they do it in a way that maintains as much normalcy for face-to-face students as possible. Teachers have been asked to avoid spending excess time troubleshooting technology or otherwise disrupting their normal teaching activities in support of online learners. Disruptions are to be expected, however, teaching as many students as possible in the time allotted to each class will drive teachers' actions.

Visitors to the digital classroom should treat the interactions as if they were visiting a classroom in person. While parents are welcome to sit in on digital classes and some troubleshooting is inevitable, we ask that parents minimize their involvement. Recognize that teachers may be self-conscious about having visitors watching the live video feed. Online classes are not an opportunity to criticize or interfere with teaching practices. Please remain positive, respectful, and supportive of our faculty, as we tackle the challenges of concurrent in-person and online teaching.

As several factors are beyond the control of Rivermont, please recognize that disruptions to the distance learning experience are to be expected. Please feel free to troubleshoot and coordinate with teachers after the class has ended, preferably via e-mail. If you want to speak with a teacher, please e-mail and set an appointment to do so, as they are working hard to make things work as well as possible, for everyone. If technical support is required that the teacher is unable to help solve, please contact our technology support person, Melissa Sweeny, at msweeny@rivermontcollegiate.org.

Privacy and Visitors to the Digital Classroom

Parents and students engage in Rivermont Collegiate's programs voluntarily through the enrollment process. In so doing, it is understood that all members of the community agree to and will be held accountable to Rivermont's policies. This applies to both face-to-face, as well as digital interactions. Great efforts are taken to ensure that our data is secured and distributed only within its community. The school and its teachers are operating in good faith and adopting policies and practices amidst changing laws and guidance, amidst the global pandemic and shifting local and geopolitical travel restrictions.

Rivermont uses a password-protected Microsoft Office TEAMS platform for its e-mail, document storage, and web streaming services, while RenWeb, another secure platform independent of TEAMS, hosts our assignments and grades. Both feature excellent privacy safeguards, are password-protected, and administered by Rivermont for use within its community only. Copyrighted material may be shown in the live streaming classes and recordings thereof, in a manner consistent with copyright law.

Teachers have been asked to be mindful that some student information is private, while other information is protected entirely, and to act accordingly. Nevertheless, teachers will be using students' names and students' likenesses, which may appear in the video feeds of live-streamed classes, as well as recordings thereof. The Data Definition and Ownership policy below is intended to protect both students, as well as Rivermont and its faculty from misuse or unlawful retention or distribution of any data.

Additional Guidelines

The Rivermont Collegiate Network is intended to enhance the educational resources of the School. The goal is to facilitate access to resources, improve communication, and encourage innovation. Your school-issued or personal device is an academic learning tool which provides ubiquitous access (wired and wireless) to an array of programs and tools. Use of technology at School is a privilege, and its benefits are highly dependent on an atmosphere of mutual respect and trust as you explore the digital world.

It is the expectation of the School that students will behave in a lawful, ethical, and respectful manner. There is no expectation of privacy when using the School's network. If a violation of this policy is suspected, private files or correspondence may be investigated, and social media sites may be monitored. It is important to recognize that behavior both on and off campus reflects on the reputation of the School. Failure to act responsibly may result in disciplinary consequences such as loss of e-mail privileges, loss of Network and Internet access, detention, suspension from athletic participation, suspension, or, in extreme cases, expulsion; or any other action the School deems appropriate. Rivermont Collegiate will cooperate with any law enforcement agency in the event of suspected illegal or inappropriate activities.

Rivermont Collegiate recognizes the value and potential of personal publishing in media and on the Internet; however, discretion should be exercised in any posting or publishing in media or on the Internet regardless of the computer or network that is being used. It is an expectation that a member of the Rivermont Collegiate community will not use the School name, its nickname, or symbol in any media content that is in conflict with the School's policies and standards for responsible behavior. This includes but is not limited to drug and alcohol references; prejudiced or discriminatory speech; reference to violent or illegal behavior; obscene pictures or language; assuming another person's identity; or language that is unsportsmanlike, demeans, libels, bullies, threatens, or harasses another individual or group.

Postings on the Internet are public and permanent, regardless of privacy settings, so at no time are students to provide identifying or incriminating information that could put the School community at risk. In general, students should not be posting any material on social media sites that they would not want their parents, teachers, college admissions officers, or potential employers to see.

Remote Learning Platform

Student/Parent Rights and Obligations

1. Parents and students are obliged to abide by all legal requirements (such as a declaration for consent of the parents in the case of minors) and administrative procedures in place for students and parents to access Rivermont's remote learning platform; parents and students agree to perform all necessary actions in order to fully comply with applicable legal requirements and administrative procedures.
2. Parents and students shall ensure all necessary technical conditions for the successful use of the remote learning platform, thus meeting the requirements of Rivermont [as specified in the Technical Requirements and Support Policy].
3. Parents and students are obliged to use the remote learning platform personally strictly for educational purposes of Rivermont students and parents. Parents and students are not allowed to share or transfer their right to use the remote learning platform to any third party; any such sharing or transfer is strictly prohibited.
4. By using the remote learning platform, Rivermont parents and students represent, warrant and agree no materials of any kind submitted through the platform or otherwise posted, transmitted or shared by students or parents on or through the platform will violate or infringe upon the rights of any third party, including copyright, trademark, privacy, publicity or other personal or proprietary rights; or contain libelous, defamatory or otherwise unlawful material.
5. Students and parents agree and declare they will not use the platform to:

   a. Post content or initiate communications that are unlawful, libelous, abusive, obscene, discriminatory, invasive of privacy or publicity rights, hateful, or racially, ethnically, or otherwise objectionable;

   b. Upload, post, email, transmit, or otherwise make available any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation;

   c. Harvest or collect email addresses or other contact information of other students or parents from the platform by electronic or other means for the purposes of sending unsolicited emails or other unsolicited communications;

   d. Use the platform in any unlawful manner or in any other manner that could damage, disable, overburden or impair the platform or Rivermont;

   e. Falsely state, impersonate, or otherwise misrepresent student or parent identity, including, but not limited to, the use of a pseudonym, upload, post, transmit, share, store, or otherwise make publicly available on the platform any private information of any third party, including, without limitation, addresses, phone numbers, email addresses, Social Security numbers, and credit card numbers;

   f. Upload, post, transmit, share or otherwise make available any material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment;

   g. Intimidate or harass another person or entity; or

h. Post, modify, distribute, or reproduce in any way any copyrighted material, trademarks, or other proprietary information belonging to others without obtaining the prior written consent of the owner of such proprietary rights.

6. Parents and students recognize the global nature of the internet and agree to comply with all applicable local rules including but not limited to rules regarding online conduct and acceptable content. Specifically, parents and students agree to comply with all Rivermont policies and applicable laws regarding the transmission of data.
7. In cases of any third party claims against Rivermont regarding actions of students or parents, the parent or student is obliged to bear all legal, administrative and other costs related to such claims, including to indemnify and hold harmless Rivermont for any such claims, including Rivermont's attorney fees.
8. In cases of default by a parent or student regarding the foregoing provisions, Rivermont is entitled to terminate the parent's or student's use of the platform without prior notice.

Bring Your Own Device (BYOD) Policy - Devices not owned by the School

Device Types

For the purpose of this program, the word "device" means a privately owned wireless and/or portable electronic piece of equipment that includes laptops, netbooks, tablets/slates, iPod Touches, cell, and smartphones.

Guidelines

1. Any student using a personally owned electronic device at Rivermont Collegiate must read and sign this agreement and submit to the division administration.
2. The student takes full responsibility for his or her device and keeps it with himself or herself at all times. The School is not responsible for the security of the device.
3. The student is responsible for the proper care of their personal device, including any cost of repair, replacement, or any modifications needed to use the device at School.
4. The School reserves the right to inspect a student's personal device if there is reason to believe that the student has violated Board policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device.
5. Violations of any Board policies, administrative procedures, or school rules involving a student's personally owned device may result in the loss of use of the device in School and/or disciplinary action.
6. The student complies with teachers' request to shut down the computer or close the screen.
7. Personal devices shall be charged prior to bringing it to School and shall be capable of running off its own battery while at School.
8. The student may not use the devices to record, transmit or post photos or video of a person or persons on campus without administrative permission. Nor can images or video recorded at School be transmitted or posted at any time without the express permission of a teacher.
9. The student should only use their device to access relevant files.
10. The student will use the Rivermont wireless network. Use of 3G & 4G wireless connections is strongly discouraged as Rivermont Collegiate cannot provide security protection on personal networks.

Rivermont Collegiate BYOD FAQs – Parents

What type of device(s) should my student have for School? What hardware/software should the device be equipped with?

Rivermont suggests a laptop with a full keyboard equipped with Windows 10 and an Intel Core i3, or better, processor. A built-in webcam is strongly recommended. An iPad or Tablet is NOT recommended. Rivermont will install Microsoft Office if the software is not already on the device.

What about antivirus software?

It is the responsibility of the owner to install antivirus protection on personal devices.

What if my child's device is stolen or damaged? What recourse can I take?

Students bring electronic communication devices to School at their own risk, just like any other personal items. Rivermont will not be held responsible if an electronic device or other item is lost, stolen or misplaced. Some devices have a device locator; it is recommended that you enable this feature if possible.

Is it required that my child use the School wireless? Can they use their own 3G or 4G service?

Students with a personally owned device need to use the Rivermont wireless network, as that network has filters in place for student protection.

My child is bringing a device to School for instructional purposes. Will they have access to things they normally do with school equipment?

Your child will have access to any of the web-based or networked software the School currently uses (databases, library search tools, etc.) Software may run differently on different devices for varying reasons.

How will my son's/daughter's device be used in the classroom?

Schools must challenge students with rigorous, personalized academic learning experiences that foster innovation and creativity. Students will engage in a cohesively integrated curriculum, access information, and apply it to solve authentic problems in a collaborative manner.

Rivermont Collegiate BYOD FAQs – Students

I have my device with me in class. How do I get on the Internet now?

Most devices will detect a wireless connection when you are near one. Most of the time, devices will ask you if you would like to join the network when prompted, choose RVMT from the list. If you need assistance, check with a member of the IT department.

I can't get my device to connect to the network. Can I get some help from someone?

Resources may be available to help you connect to the RVMT network at School; however, you will need to consult with a network administrator for these resources. It is not the responsibility of your teacher or other staff to troubleshoot individual devices during the school day. It is recommended that you check with a member of the technology team for assistance.

I need to save my work. How do I do this?

When you choose "Save As", select your OneDrive account as your file destination. You can also save work using a flash drive, your own hard drive, or a course management system.

My device was stolen when I brought it to School. Whom should I contact about this?

It is always a good idea to record the device's serial number to have in case of theft or lost items. Rivermont Collegiate is not responsible for the theft of a device, nor are they responsible for any damage done to the device while at School. Any time a theft occurs, you should contact a school administrator to make him/her aware of the offense.

Why am I filtered on my own computer? Shouldn't I be able to see what I want to on my own device?

Internet filtering is a requirement of all schools. The Children's Internet Protection Act (CIPA) requires all network access to be filtered regardless of the device you use to access it while at School. You own your device, but the network you're using belongs to the School, and Internet access will be filtered.

COPPA (Children's Online Privacy Protection Act)

Verifiable Parental Consent

In order for Rivermont Collegiate to continue to be able to provide students with the most effective web-based tools and applications for learning, we need to abide by federal regulations that require a parental signature as outlined below. Rivermont Collegiate utilizes several computer software applications and web-based services, operated not by Rivermont Collegiate, but by third parties.

In order for our students to use these programs and services, certain personal identifying information, generally the student's name and school e-mail address must be provided to the web site operator. Under federal law, these web sites must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. The law permits schools such as Rivermont Collegiate to consent to the collection of personal information on behalf of all of its students, thereby eliminating the need for individual parental consent given directly to the web site operator. This form will constitute consent for Rivermont Collegiate to provide personal identifying information for your child consisting of first name, last name, and/or e-mail address and user name to the operators of any additional web-based educational programs and services which Rivermont Collegiate may utilize during the academic year.

As a Rivermont Collegiate Student, I Agree To:

- Practice responsible, balanced, and healthy use of technology both at School and at home.
- Be solely responsible for the use of my own account both on and off campus, before, during, or after the school day.
- Maintain the privacy of self and others.
- Always treat others in a respectful, positive, and considerate manner.
- Represent the School in a positive light.
- Honor division, grade level, and classroom rules about inappropriate games, software, and instant messaging.
- Adhere to copyright laws, licensing agreements, and terms and conditions of use.
- Be aware that technology is a shared resource and conserve the limited shared resources of the Rivermont Collegiate network and technology equipment (for example, by not streaming music or videos unrelated to school assignments).
- Report misuse of the technology of others and the Rivermont Collegiate network and technology equipment.
- Abide by further guidelines set by individual faculty for technology use in classes and public spaces.

As a Rivermont Collegiate Student, I Agree NOT To:

- Share personal passwords or other private information about my account.
- Use another person's account, files, or passwords with or without their permission.
- Share personal or identifying information about any member of the School community.
- Use inflammatory, unsportsmanlike, derogatory, threatening, obscene, or pornographic language or pictures.
- Engage in cyberbullying, including harassing, denigrating, outing, tricking, excluding, and cyberstalking.
- Impersonate others or re-post comments without permission of the original sender.
- Access or post information to inappropriate sites from devices on the wired or wireless Rivermont Collegiate Network.
- Attempt to circumvent any web filters or safety measures blocking access to any sites.
- Alter, destroy, or obstruct the settings, configurations, or resources of the Network.
- Connect any other equipment such as printers, routers, or servers to the Network or install personal software on the Network or workstations without permission.
- Engage in activity that is illegal or for personal profit.

This is not intended to be an exhaustive list. Students should use their own good judgment at all times.

References:

School Code – 24 P.S. Sec. 1303.1-A

PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.

Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256

Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777

Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254

Children's Internet Protection Act Certifications, Title 47, Code of Federal

Regulations – 47 CFR Sec. 54.520

Technology Acceptable Use Parent Signature Page

As parent or legal guardian, I have read this Technology Acceptable Use & COPPA Policy and have discussed it with my child.

I grant permission for my student to use a personal and/or school-owned computing device while at Rivermont Collegiate and to have access to the Rivermont Collegiate network (wired and wireless), Internet, and school software. I grant permission for my student to utilize his/her school e-mail account (provided by Rivermont) for school assignments and projects. I understand that my child's school e-mail account will be restricted so that it can only send/receive within the Rivermont domain.

I understand that it is impossible for Rivermont Collegiate to restrict access to all controversial materials and will not hold the School responsible for materials acquired on the Internet. I understand that my child will face disciplinary action if she violates the Rivermont Collegiate Technology Responsible Use Policy, whether that misuse occurs on campus, or off, on School computers, or on technology that is privately owned.

Student Name____________________________________ Grade___________

Student Name____________________________________ Grade___________

Student Name____________________________________ Grade___________

Student Name____________________________________ Grade___________

Student Name____________________________________ Grade___________

____

Parent Signature Date