Diocese of Baton Rouge Catholic Schools Office
Technology Acceptable Use Policy
Effective Date: July 1, 2022

A key purpose of this document is to serve as the basis for the inclusion of a Technology Acceptable Use Policy in the parent/student handbook of each of the Catholic schools (each a "**School**" and collectively, the "**Schools**") within the Diocese of Baton Rouge (the "**Diocese**").

Statement on Technology

The mission of the Technology Department at each of the Schools within the Diocese is to provide a range of technology services, tools and experiences to further opportunities for academic excellence, faith development, and leadership skills. Technology is used to support, enhance and optimize the learning process for all of our students. Emerging technologies will influence the formation of foundational skills in students to aid them in reaching their potential in a constantly changing world. Technology must be implemented seamlessly, as everyday experiences, and must promote higher student achievement and a deeper understanding of their Catholic faith. Technology use within our Schools shall be consistent with the mission and vision of the Diocese to evangelize hearts, educate minds, encourage talent, and embrace the future.

This Technology Acceptable Use Policy ("**AUP**") contains terms, conditions and standards ("**Standards**") that foster our mission and goals. By using any technology, equipment, or resources of a School or the Diocese as contemplated herein, the individual user is deemed to agree to be bound by this AUP and to strictly comply with all Standards contained herein. This AUP is reviewed annually to reflect any new technology and to address issues identified in the previous year. Each academic year, all students and parents at a School within the Diocese must read and contractually agree to abide by these Standards. Any student who violates this AUP or any applicable local, state, or federal law, is subject to disciplinary actions, including but not limited to a loss of technology privileges, potential legal liability to the School and/or Diocese, and potential legal prosecution at the discretion of local law enforcement.

As technologies continue to evolve, so will this document. The Diocese and administration of each School reserve the right to amend any item in the AUP or any technology policy during the year. Schools will notify parents and students in writing should any changes in this AUP occur during the school year.

Scope of Use

We recognize that the digital world allows anytime, anywhere access. School hardware, software, and technology services are provided for faith and academic purposes. All students using said technology shall be accountable for its use. Students are expected to use all technology resources in a considerate, ethical, moral, and legal manner, ensuring their actions are consistent with the School's Code of Conduct, which guides student behavior both on and off campus. Any potential or actual threat to the School, or the individuals contained within it, shall be viewed as a violation of this AUP and those individuals may be subject to the disciplinary measures found herein.

The types of electronic and digital communications referenced in this AUP include, but are not limited to, social networking sites or applications ("**apps**"), collaborative tools, cell phone calls, voicemails, voice memos, digital cameras, text messaging, email, Voice over IP, chat rooms, message board posting, blog or article comments, and instant messaging.

Device Usage

For purposes of this AUP, the term "**device**" includes, without limitation, cellular telephones, smart phones, personal and School-owned/issued computers, laptops, tablets and similar devices.

Privacy

All electronic resources owned or issued ("**owned/issued**") by a School remain the property of the School unless otherwise agreed to in writing. The individual has no reasonable expectation of privacy. The School retains the right to monitor any and all electronic resources, including personal devices as part of a "Bring Your Own Device Program" (BYOD).

Each School-owned/issued technology device/accounts and the information stored on it are property of the School and are subject to the policies set forth by School administration and are subject to supervision and inspection. The Diocese and each individual School reserves the right to monitor, access, retrieve, read, and disclose any and all messages, information, and files created, sent, posted from, and/or stored on any School-owned/issued device/account.

General Computer and Internet Usage

At times, students will have access to varied types of electronic and virtual resources to complete educational tasks, including but not limited to storage, network communications, equipment, apps, and software.

Technology devices and resources usage is a privilege, not a right, which may be suspended, revoked or terminated in whole or in part and with or without notice by the School or Diocese, in its/their sole discretion, upon any actual or alleged violation of this AUP. By using such devices and resources, parents, and students are deemed to agree to the following terms:

- Students shall not download or install software or third-party applications on any School-owned/issued device which may interfere with the educational process (e.g., games) or which change a device's system configuration without specific instruction from their teacher.
- Students shall not attempt to gain unauthorized access to or compromise any computer or network security or engage in any illegal activities on the internet, including but not limited to, willfully introducing a computer virus, worm, or other harmful program.
- Use of a School's network and internet usage must be consistent with the mission of the Diocese and the School and of the educational goals of each. Misuse includes, but is not limited to, any of the following: (i) any internet conduct on or off School campus which reflects negatively on the Diocese and/or School or the educational goals of each, including but not limited to sending or posting photos, images, videos, messages, or other communications that contain or suggest harassment, racism, sexism or inappropriate language and/or symbols; and, (ii) sending, transmitting or displaying any unchristian, immoral, offensive, violent, pornographic, obscene or sexually-suggestive or explicit photos,

images, videos, messages, or other communication in any form. Any such misuse, as determined by the School and/or Diocese in its/their sole discretion, is strictly prohibited.

- Any student who receives a message suggesting harassment, racism, sexism or the contents of which include inappropriate language, images, and/or symbols must immediately report it to a teacher, counselor, or administrator.
- Any failure by a student to immediately make known to a teacher or an administrator at the School that the student received a message which suggests harassment, racism, sexism or contains inappropriate language, images, and/or symbols will constitute misusing technology.
- If a student has access to network resources or internet access, the student will not disrupt network users, services, equipment, or data of the Diocese, any School, or another student, whether on or off campus.
- Students will not attempt unauthorized entry to any device accessible via the School network or remote network. If a student notices what is or may be a security concern, the student must notify administration immediately.
- The internet contains certain material that is illegal, defamatory, inaccurate or potentially offensive to some people. Students will not use network resources or internet access to knowingly visit sites that contain such material nor import, transmit and/or transfer any such material to other computers.
- Students shall not capture or transmit any image, video, or audio of School employees. Photographing and/or recording (by audio and/or video) a teacher, staff member, student, or any other individual without permission of the subject is prohibited.
- Students will not provide their password(s) or access code(s) to, or share another student's password(s) or access code(s) with, any other student or nonstudent. Students shall not use another individual's device/account or log onto the internet or network as anyone other than themselves.
- Students are responsible for all digital data, activity, and products on their School-owned/issued devices/accounts.
- Students shall observe all intellectual property laws and fair use guidelines (e.g., copyright, trademark, licensing and similar laws, rules and regulations). Copying, modifying, distributing, displaying, or transmitting the work of another without written permission or proper citation is prohibited.
- Students will not communicate the address, phone number, or other personal information of themselves or any other individual to any person or legal entity on the internet or through email without specific instructions from their teacher or administrator.
- While using any technology device at School, students are required to access the internet using the School's Wi-Fi and are prohibited from connecting to secondary Wi-Fi devices, such as a cell phone and/or other external devices. The Children's Internet Protection Act (CIPA) laws require the Schools to filter internet access to students and block inappropriate content from being accessed. This prohibition includes internet tethering and mobile hotspots that enable cellular data access on the School-owned/issued laptops.
- Content filtering alerts received by School personnel outside of normal school hours will be addressed the following school day.
- Student use of a Virtual Private Network (VPN) is prohibited at any time.

- The intentional destruction, deletion, or disabling of School-installed software on any device is prohibited. Unauthorized copying/installation of software programs belonging or licensed to a School is prohibited. Also, attempts to exceed or modify the boundaries set for the network are prohibited.
- Deleting, examining, copying, or modifying files and/or data belonging or licensed to a School is prohibited, unless specific instruction is given by a teacher for changes related to non-sensitive files/data.
- Purposeful or careless damage to School-owned/issued devices is prohibited. Each individual user will be responsible for any repair or replacement costs (at then-current rates, including associated taxes and third-party charges) and commercially reasonable administrative or replacement fees as set by the School. The School has the discretion to suspend each user's technology privileges and/or take disciplinary action.
- Students shall not dispose of any School-owned/issued device without the prior approval of the School. Any such disposal of a School-owned/issued device shall be conducted by the School or, if directed by the School, by the student in accordance with the School's directive. Prior to leaving School enrollment, if directed by the School, students must return all School-owned/issued devices.
- In the case of theft of a School-owned/issued device, parents are required to notify the School and file a police report within 24 hours of becoming aware of it. Misplaced/lost devices must be reported to School personnel immediately. If the device is not recovered, the student's parent/guardian is responsible for the replacement cost of the device.

Email and Communication Use

Some Schools within the Diocese will issue to students password-protected logins for the network, School email, and other electronic communication resources. Not all Schools will provide this access.

For Schools which do have email accounts and other means of electronic communication for their students:

- Written parental permission is required for a student to have the use of a School-issued email account.
- Instant messaging, chat rooms, social networking, gaming, email, and other electronic communication between students for non-academic purposes are prohibited unless these activities are directly related to class activities and/or participation and are within the scope authorized by School faculty.
- Students shall not change their given email usernames.
- All communications sent or received may reflect on the Diocese, School, and the applicable church parish; thus, communication exchanged via the internet or email must not damage the reputation of the Diocese or School as determined by it/them in its/their sole discretion. No such communications shall be made for personal gain, to solicit others for activities unrelated to School-approved purposes, or in connection with political campaigns.
- All email communication between faculty, staff, coaches, and one or more students must be exchanged through the School-issued email account. Others, such as volunteer coaches, who are not School employees or administrators but who otherwise participate in School

academic, athletic or other extra-curricular activities, may be granted access to a School-hosted email account at the School's discretion, in which event the School-hosted email account shall be used only for School purposes and shall be subject in all cases to the terms, conditions and standards of this AUP and such users, upon request, shall contractually agree to abide by Standards set forth herein. If a School-hosted email account is not granted, all such individuals will nonetheless send email communication only to School-hosted email accounts when intended for School faculty, staff, coaches and students.

- Students are responsible for reporting and rejecting any inappropriate materials and information received through electronic communication.
- Students are prohibited from attempting to access or using another student's email account.
- Students will not use network resources or internet access to broadcast messages via the School's network or email system, or to transmit threatening, obscene or harassing materials, including but not limited to chain-letters, solicitations, inappropriate images, and videos.
- The Diocese and School each reserves the right to access student email accounts at any time. This reservation includes, but is not limited to, access of the student's email account for routine maintenance and to retrieve School records. Such access also includes, but is not limited to, carrying out internal investigations, accessing internet history, and the disclosure of messages, social networking data or files.
- School employees may share any information obtained in a search of a student's email account with law enforcement as deemed necessary by the School administration at their discretion.
- Instant messaging, chat rooms, social networking, gaming, and email communication between students for non-academic purposes are prohibited unless these activities are directly related to class activities and/or participation.
- Prior to leaving School enrollment, students shall return all School-issued e-mail and user accounts. The School reserves the right to deactivate any such accounts at any time following unenrollment.

Cellular Devices

The Diocese recognizes the convenience, logistical and safety advantages for students to have cellular telephones and other communication devices in their possession while on campus and during School activities.

- Communication devices are to be used in accordance with School policy and must not disrupt the educational environment.
- Students may use communication devices while on School campus and during School activities only with the permission of the supervising adult, such as the teacher, bus driver, athletic coach or sponsor, and only within the scope of such permission.
- The use of communication devices in an unacceptable manner in the School setting is prohibited. Examples of unacceptable usage include, but are not limited to, the following: use of a device for any purpose inside a restroom or locker room, use of a device on the School campus for cheating, cyber bullying, sexting, and taking inappropriate photos or videos.
- Violations of this AUP may result in disciplinary measures as well as the confiscation of the communication device.

Personal Devices

Each School shall determine whether personal devices are permitted on its campus, including but not limited to Fitbits, Smart watches, or other wearable technology, tablets, computers, and cameras. To the extent so permitted by the School, such items will constitute a device for purposes of this AUP, and any such permitted use shall be subject to all of the terms, conditions and standards of this AUP.

Conflicts

Individuals subject to this AUP may also be subject to other School or Diocesan policies with respect to communications, the use of technology, or other matters covered by this AUP (each an "**Other School Policy**"). This AUP is not intended to modify any Other School Policy, nor should any Other School Policy be construed to modify any term, condition or provision of this AUP. In the event of a conflict between any term, condition or provision of this AUP and any term, condition or provision of any Other School Policy, the more restrictive user term, condition or provision shall apply.