

**Diocese of Baton Rouge Catholic Schools Office**

**Technology Acceptable Use Policy**

The intention of this document is to serve as the basis for individual school’s Acceptable Use Policy to be included in the parent/student handbook of each school. [Note: This document may be adapted or amended to suit the needs of each school within the Diocese of Baton Rouge without substantial changes to the integrity of the policies.]

**Statement on Technology:**

It is the mission of the Technology Departments at each of the schools within the Diocese of Baton Rouge 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.

This Acceptable Use Policy (AUP) contains standards that foster our mission and goals. The policy is reviewed yearly to reflect any new technology and to address issues identified in the previous year. Each year, all students and parents at a school within the Diocese of Baton Rouge must read and agree to abide by these standards. Any student who violates this policy or any applicable local, state, or federal laws is subject to disciplinary actions, a loss of technology privileges, and may face legal prosecution. The Diocese of Baton Rouge and administration of each school within the Diocese of Baton Rouge reserve the right to amend any item in the AUP or any technology policy during the year. Parents and students will be notified of any changes through normal methods of communication at each school.

**Privacy:**

All electronic resources 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 all electronic resources in any manner it sees fit.

Any person using school owned/issued technology devices is expected to use all technology resources in a considerate, ethical, moral and legal manner.

Any school owned/issued technology device and the information stored on them 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 of Baton Rouge and each individual school reserve the right to monitor, access, retrieve, read and disclose all messages, information, and files created, sent, posted from, and/or stored on any school owned/issued device.

**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. By using such devices

and resources, parents and students agree to the following terms:

* Students are not allowed to install third party applications on the school owned device which may interfere with the education process (e.g., games) 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 willfully introducing a computer virus, worm, or other harmful program.
* Student use of the school’s network and internet usage must be consistent with the mission of the diocese and the individual school and of the educational goals of both. Misuse includes any internet conduct on or off campus which negatively affects the reputation of the diocese and/or school and the educational goals of both. This includes but is not limited to sent or posted messages that suggest harassment, racism, sexism or inappropriate language and/or symbols.
* Any student who fails 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 has inappropriate language, pictures, and/or symbols will be considered to be 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, the school, of another student, either 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 a security problem, 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 this material nor import, transmit and/or transfer any of this material to other computers.
* Students may not email or post to websites or blogs any images, photos or videos of school employees. Photographing and/or recording (audio or video) a teacher or staff member without permission is prohibited.
* Students will not provide their password(s) or share another student’s password with any other student or nonstudent. Students may not use another individual’s account or log onto the internet or network as anyone else.
* Students shall observe copyright laws and fair use in guidelines. Copying, modifying, distributing, displaying, or transmitting the work of another without 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 company on the internet or through email without specific instructions from their teacher.
* 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. Children’s Internet Protection Act (CIPA) laws require schools to filter internet access to students and block inappropriate content from being accessed. This includes internet tethering and mobile hotspots that enable (3G or 4G) access on the school issued laptops.
* The intentional destruction, deletion, or disabling of school - installed software on any device is prohibited. Unauthorized copying/installation of software programs belonging to the 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 to the school is prohibited, unless specific instruction is given by a teacher for changes related to non-sensitive files/data.
* Purposeful damage to school issued or owned devices is prohibited. The individual will be responsible for any repair or replacement costs. The school has the discretion to suspend the user’s technology privileges and/or take disciplinary action.

**Email and Communication Use:**

Some schools within the Diocese of Baton Rouge will issue password protected logins for the network, school email, and other communication resources to students. Not all schools will provide this access.

For schools which do have email accounts for their students:

* Parents will be required to specifically acknowledge the use of the email account by their child.
* Students may not change their given email username.
* All communications sent or received serve as a representation of the diocese, parish, and school, as communication exchanged via the internet or email must not damage the reputation of the diocese or school.
* All email communication between faculty, staff, coaches and a student must be exchanged through the school-hosted email account.
* Students are responsible for reporting and rejecting any inappropriate materials and information received through electronic communication.
* Students are prohibited from attempting to access or otherwise use 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 photos and videos.
* The Diocese of Baton Rouge and/or the student’s school reserve the right to access student email accounts. This includes but is not limited to access of the student’s email account for routine maintenance and to retrieve school records.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 student email accounts with law enforcement as deemed necessary by the school administration.
* 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.

**Device Usage:**

For purposes of this policy, the term device includes, cellular telephones, personal and school issued computers, laptops, tablets or similar devices.

**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 must be turned off and stowed away throughout the academic day, during school activities, and may not be displayed.
* Students may use communication devices while on campus and during school activities only with the permission of the supervising adult, such as the teacher, bus driver, athletic coach or sponsor.
* The use of cellular devices in an unacceptable manner in the school setting is prohibited. Examples of unacceptable usage can include but are not limited to the following: use of a device for any purpose inside a restroom, use of a device on the school campus for cheating, cyber bullying, sexting, and taking inappropriate pictures or videos.
* Violations of this policy will result in disciplinary measures as well as the confiscation of the communication device.

**Wearable Technology:**

It is up to the individual school whether or not smart watches, Fitbits or other wearable technology are permitted.

**Personal Devices:**

It is up to the individual school whether or not personal devices are permitted at school.