

Sacred Heart School  
Technology Acceptable Use Policy Guidelines

## **Purpose of Technology Use**

Sacred Heart School provides technology resources to its students solely for educational purposes. Current and expanding technologies allow teachers to take students beyond the confines of the classroom and provides opportunities for enhancing, extending and rethinking the learning process. It is our belief that access to technology promotes educational excellence through resource sharing, innovation and communication with the support and supervision of parents, guardians, teachers and staff.

## **The Opportunities and Risks of Technology**

At Sacred Heart School we believe in the benefits of a 1:1 device program. When students have access to their own device, teachers can communicate seamlessly, adapt better to learning styles and can personalize assignments. Access to technology also provides increased creative outlets and prepares our students to be future ready. We believe that the educational opportunities provided through a 1:1 device program outweigh the potential risks. To best support our students with online safety, Sacred Heart subscribes to GoGuardian software. GoGuardian provides content filtering and monitoring services to every student issued a Chromebook. It is important to note that web filtering software cannot completely guarantee blocking access to materials deemed harmful, indecent, offensive or otherwise inappropriate. The use of filtering software does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

## **Privileges and Responsibilities**

The content accessed online is part of the Sacred Heart School curriculum and is not intended for general use. Student users are responsible for their behavior and communications while on our in-school network and online while at home.

Student users of technology shall:

- Use or access online resources for educational purposes only
- Understand that email and onboard files are not private. Network administrators may review files and communication for responsible student use.
- Respect the privacy rights of others
- Be responsible with the proper use of access privileges. Students should only work under their username and login. At no time should a student share any code or password.

Students should not improperly represent themselves online. Improper representation includes, but is not limited to:

- Any and all illegal purposes
- At no time should a student retrieve or view obscene or explicit material
- While online, students shall not discriminate, harass or bully individuals based on race, gender, religion, orientation or disability
- Any use of profanity, obscenity or language that is offensive or threatening
- Reposting or forwarding personal communication without the author's consent
  - This includes synchronous or asynchronous Zoom or other video conferencing
  - Chat, email or any other correspondence
- Reposting or forwarding of junk mail, chain letters, or inappropriate or offensive jokes
- Hacking of any kind, including, but not limited to illegal or unauthorized access
- Soliciting or distributing information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.

## **Disciplinary Actions**

Violations of this policy may result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion or other appropriate disciplinary action.

## **Internet, social media, online gaming and YouTube Safety**

Through careful consideration, the administration and faculty at Sacred Heart School does not recommend that any student under the age of 13 have a personal social media account. Parents/guardians should be aware of the potential risks to children who engage in social media, YouTube or online gaming. The risks include, but are not limited to:

- being exposed to inappropriate or upsetting content like mean, aggressive, violent or suggestive comments or images
- uploading inappropriate content like embarrassing or provocative photos or videos of themselves or others
- sharing personal information with strangers
- cyberbullying
- exposure to too much targeting advertising and marketing
- having personal data sold on to other organizations

Students and families should take steps to ensure child safety while online.

- Students should not give out identifying information (home address, school name or phone number) to others on the the Internet
- Students should not arrange a face-to-face meeting with someone they meet while online without parental/guardian permission.

- Student users should not respond to messages that are suggestive, onscene, threatening or make a student feel uncomfortable. If a student receives such a message, he/she should provide a copy of the message to a parent/guardian immediately.

Families should also consider the addictive nature of the various applications used through smartphone and tablets. Parents/guardians should be aware that smartphones and tablets can:

- create a dependence by their users and may produce addictive brain responses
- are an academic distraction
- can impair sleep
- can put your child at risk for cyberbullying
- can increase the risk of anxiety and depression
- can interfere with personal relationships

We understand that family dynamics play a role in smartphone and online participation. For families with younger students, we ask that they at least explore the Wait Until 8th initiative. The Wait Unit 8th pledge empowers parents and families to rally together to delay giving children a smartphone until at least 8th grade. Please explore the website for more information and to take the pledge:

<https://www.waituntil8th.org/>

## Program Agreement

I have read the above AUP agreement and will abide by the terms and conditions and this agreement.

---

Parent Signature

---

Date

---

Student Signature

---

Date