

## **Diocese of Oakland Technology Responsible Use Policy Students and Parents**

### **Introduction**

The Diocese of Oakland recognizes the various ways, both positive and negative, that students and parents can use technology both in school and at home. Our objective is to fully prepare students to use the resources available in ethical, constructive, productive and intelligent ways as Christian citizens in a global community.

Students are expected to abide by the student responsibilities below anywhere or anytime their actions can affect the school or other students. While the school is not responsible for policing online activity, conflicts online between students, parents, or staff rarely stay online; the school is notified when such conflicts affect the wellbeing of members of the school community. Students and parents who use technology in ways that are contrary to our mission will face disciplinary action, up to and including expulsion.

### **Jurisdiction and Definitions**

While using technology, students are expected to comply with the code of conduct published in the school's parent-student handbook. The school's jurisdiction with respect to conduct includes:

- When the student is on school grounds, or on the way to or from school
- At officially sanctioned school-sponsored events, or on the way to or from such events
- Outside of the school when a student's actions negatively impact another student, staff member, or the school

For purposes of this document, "technology" includes, but is not limited to:

- Hardware: computers, servers, tablets, e-Readers, phones, smartphones, digital cameras, gaming devices, wearable devices (watches, headphones, etc), networking equipment, or accessories
- Software: operating systems and programs
- Services: email, web sites, web apps, learning platforms, internet service
- Telecommunications: transmission or publishing text messages, chat room commentary, comments, pictures, videos, audio recordings, posts on social networking sites, blogs, wikis, gaming, chats, and other digital transmissions.

"Personal information" includes a person's name, address, email addresses, phone numbers, online accounts, or other contact or identifying information.

### **School Responsibilities**

#### **Protecting student data**

The school maintains electronic records and shares information from those records in order to provide online educational technology services. Electronic records allow the school to efficiently distribute information to school officials - such as teachers receiving parent phone numbers and email addresses - and to online services. For example, the application Mathletics receives each student's name, grade level, gender, and email address, used to set up their account. The school only uses services that have high standards for security and privacy, and do not sell or share student data. Most have signed the Student Privacy Pledge ([studentprivacypledge.org](http://studentprivacypledge.org)). Parents may request a review of services in use by the school.

Initial:  The school may store and share student information electronically for purposes of distributing that information to school officials and providing educational technology services.

#### **Efforts to protect students online**

Internet within the school is filtered with the intent to block access to obscene and non-educational material. In addition, the school has adopted and enforces an Internet safety policy to monitor network activity, promote safe communications, educate students in Digital Citizenship, and prevent unauthorized access to the school network and community data.

### **Parent Responsibilities**

Parents are expected to abide by the code of conduct found in the school's parent-student handbook, to the extent that their technology use affects other members of the school community.

### **Student Responsibilities**

As a member of the school community, I agree to the following rules and code of ethics:

**1. I will treat others with respect and compassion in all interactions**, including online communication. I will treat others kindly in all communications, including “private” messages. I will not publicly disparage the school, staff, students, or other members of the school community. I recognize that anything sent using technology can be copied and saved forever online.

I will not transmit inappropriate material to others via messages, social media, or other ways. Examples of inappropriate material include messages or images that are intentionally insulting, sexually explicit, racist, sexist, use foul language, depict alcohol or drug use, or include graphic violence. Such material usually upsets other students and is brought to the attention of teachers, even when sent outside of school.

**2. I will care for school devices and systems**, and not vandalize or intentionally damage them in any way. This includes hardware, software, and internet services owned, provided, or supported by the school. I will not waste school resources like paper or ink.

**3. I will respect others' privacy and work**, by protecting and not sharing or using passwords, messages, photos, recordings, or personal information of someone without their permission. I will not attempt to log into any device, program, or service as another person. I will protect and respect others' work: for other students, I will not attempt to alter or delete their work without permission. For creators who have shared their work online, I will respect copyright, abstain from piracy, and avoid plagiarism.

**4. I will use school technology resources for educational purposes only**. I will stay on task during classroom activities using technology. I will not use school devices, software, or systems (like wifi) for non-school purposes like chat, gaming, playing music or watching videos. I will not use school resources for any commercial enterprise. I will not search for material on the internet that is illegal or inappropriate for school, and if I encounter such material accidentally I will not pursue it.

**5. I will use personal technology only as directed by staff while at school**. I will only use my personal technology (including devices and internet service) at school if allowed by the school and staff. If permitted, I will use my personal technology only for educational purposes. I understand that my personal technology is still governed by this Technology Responsible Use Policy and/or the school's BYOD (Bring Your Own Device) policy. The school will not be responsible for the security, troubleshooting, charging, or repair of personal devices.

Any user who violates the Responsible Use Policy or local, state, or federal law, faces the restriction or loss of technology privileges, disciplinary action, and may face legal prosecution. Parents may be held financially responsible for any student action that results in damage to school technology or a cost to the school.

Student Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Student Name: \_\_\_\_\_

By signing below, I give permission for the school to provide technology services and for my child to use technology in accordance with the rules and code of ethics above.

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Parent/Guardian Name: \_\_\_\_\_

## **Distance Learning Addendum for 2020-2021**

The need to shift instruction during this unprecedented time requires additional safeguards and acknowledgments. As challenging as the changes of distance learning may be, we are grateful to live in an age where technology allows us to continue teaching and learning safely at home.

### **Jurisdiction**

While students are participating in distance learning, the jurisdiction of the Technology Responsibility Use Policy is expanded to include when students are at home participating in distance learning.

### **Safe and Responsible Video Conferencing and Live Streaming**

Video conferencing is a powerful tool for distance learning. Through video conferencing, teachers may deliver instruction, support students, and facilitate connections between classmates. In addition, there may come a time during the school year when some students are able to return to in-person school, while others continue distance learning. This may necessitate the use of video conferencing to “live stream” the classroom. We recognize that connecting teachers, students, and families in their homes can lead to unintended consequences. In order to maintain a positive, safe “learning environment,” school personnel, parents, and students must adhere to the following guidelines for video conferencing:

#### **School Responsibilities**

1. The school will maintain a secure video conferencing system to the best of their ability
2. The school will obtain parent or guardian consent for video conferencing with students
3. Video conferences may be recorded for instructional or archival purposes. The school will obtain parent or guardian consent before recording video conferences. Recordings will be stored securely and not published.
4. Teachers and staff will not video conference 1 on 1 with students without a parent or guardian present.

#### **Student Responsibilities**

1. Students will not take photos or recordings of video conferences
2. Students will not share links or logins for video conference meetings with anyone outside of their class community.
3. Students will attend in uniform or school-appropriate attire as directed
4. Students will inform others nearby when they are conferencing, especially when the camera or microphone is on
5. Students will attend from common areas in homes, such as the family room, dining room, or kitchen.

Initial:             I give permission for my child to participate in video conferencing with school staff and classmates.  
                        I give permission for my child’s video conferences to be recorded.  
                        I give permission for my child to appear in live streams of his or her classroom.

### **Management Tools in Distance Learning**

Some tools in use by the school can monitor or control devices. For example, GoGuardian can allow teachers to see a student’s screen or launch apps during a class session, and Chrome Remote Desktop can control a computer for tech support. These are valuable tools for educators, but they raise concerns when implemented in students homes, particularly on personal devices used for distance learning. To maintain student and family privacy, the school will not remotely operate devices without a student or parent’s consent for each support session. Monitoring data will be used only for educational purposes and to help students stay on task during the school day.

Initial:             The school may use tools to monitor, remote control, or update devices used for distance learning.

### **Internet filtering at home**

Internet on devices provided by the school for distance learning may or may not be filtered. Even when filters are enabled, it is possible for these filters to break down or be circumvented. Parents or guardians are responsible for content accessible by the internet in their homes. We recommend OpenDNS Family Shield for a simple, effective, and free home internet filter:

[opendns.com/home-internet-security](https://opendns.com/home-internet-security)

Student Printed Name: \_\_\_\_\_

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_