Internet Safety Policy
For Rock County Christian School

Introduction

It is our pleasure to be able to provide Internet access and suitable computing devices for our students and staff. We believe that doing so presents our learners and educators with the most effective opportunities to develop in today's social and professional settings. It also has the potential to present us with unholy opportunities over which each one of us needs to take authority to overcome. We choose to use these resources to better our lives, our communities, our societal norms, our economy, and our productivity. We desire to promote academic excellence through communication, understanding, and innovation through connectivity with the resources available through the medium of the Internet. And we must partner with the families to provide this safe educational environment.

We also choose to comply with the basic guidelines of the Children's Internet Protection Act to ensure the protection of our students from the harmful influences that lurk in cyberspace.

It must also be understood that all school-owned computing equipment and the technologies used to provide data communications is subject to this policy. That includes, but is not limited to:

- Desktop computers
- Servers
- Laptops
- Chromebooks
- Tablets
- Firewalls
- Switches
- WiFi Access Points
- Ethernet cabling
- Cable Modem
- Files
- Emails
- Software
- Operating Systems
- SmartBoards
- Projectors
- Displays

It is therefore the policy of Rock County Christian School to make every reasonable effort to:

1. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
2. prevent unauthorized access and other unlawful online activity;

3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.

MINOR.--The term "minor" means an individual who has not attained the age of 18.

HARMFUL TO MINORS.--The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

COMPUTER.--The term "computer" includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computing device.

ACCESS TO INTERNET.--A electronic device shall be considered to have "access to the Internet" if such device is equipped with a modem, Ethernet port, or WiFi chip or is connected via any technology to a computer network which has access to the Internet.

CHILD PORNOGRAPHY.--The term "child pornography" has the meaning given such term in section 2256 of title 18, United States Code, to wit, "any visual depiction of sexually explicit conduct involving a minor (someone under 18 years of age)".

OBSCENE.--The term "obscene" has the meaning given such term in section 1460 of title 18, United States Code, based on the following criteria:

1. Whether the average person, applying contemporary adult community standards, finds that the matter, taken as a whole, appeals to prurient interests (i.e., an erotic, lascivious, abnormal, unhealthy, degrading, shameful, or morbid interest in nudity, sex, or excretion);
2. Whether the average person, applying contemporary adult community standards, finds that the matter depicts or describes sexual conduct in a patently offensive way;
3. Whether a reasonable person finds that the matter, taken as a whole, lacks serious literary, artistic, political, or scientific value..

SEXUAL ACT; SEXUAL CONTACT.--The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code, to wit, "penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person".

TECHNOLOGY PROTECTION MEASURE.--The term “technology protection measure" means a specific technology (hardware or software firewall, cloud-based filtering service, classroom monitoring technology, etc.) that blocks or filters Internet access to visual depictions that are:

1. obscene, as that term is defined in section 1460 of title 18, United States Code;
2. child pornography, as that term is defined in section 2256 of title 18, United States Code; or
3. harmful to minors.

Access to Inappropriate Material

To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.
Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.
Subject to staff supervision, technology protection measures may be minimized only for bona fide research or educational purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Rock County Christian School online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes:

1. unauthorized access, including so-called "hacking," and other unlawful activities; and
2. unauthorized disclosure, use, and dissemination of personal identification information regarding minors in accordance with Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) regulations.

Other Inappropriate Activities

Since the classroom is established as a place of learning, it is important that we remove distractions from the immediate grasp of the students so that they may focus on those things that are more important. With this in mind, it is important that we limit access to social media and games except where it is part of the learning content, or as a reward for successful completion and comprehension of the lesson. Activities will be monitored and if a site is determined to be inappropriate by Christian standards, it will be added to the block list. Additionally, those participating in such activities will receive disciplinary consequences as outlined in the school’s Family Handbook.
Considered to be inappropriate (with exceptions made for purposes of education):

1. Violence
2. Race, ethnicity, gender, or disability degradation
3. Bullying, slandering, humiliating
4. Promotion of sinful or harmful activities including, but not limited to, drug and alcohol abuse, cutting, thievery, vandalism, occult practices
5. Use of foul or obscene language

Education, Supervision and Monitoring

It shall be the responsibility of all members of the Rock County Christian School staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the IT Director or designated representatives. As with any technology, there may be false positives and false negatives in detecting and filtering sites that should or should not be blocked. It is the right and responsibility of each teacher and staff member to contact the IT Director when modifications to the block/allow lists need to be made.

All students and their parents/guardians will be given written standards for appropriate Internet and computing equipment usage, and will be required to sign a statement of agreement to the terms of such statement before being allowed to use such resources.

The IT Director or designated representatives will provide age-appropriate training for students who use the Rock County Christian School Internet facilities. The training provided will be designed to promote the School's commitment to:

1. The standards and acceptable use of Internet services as set forth in the Rock County Christian School Internet Safety Policy;
2. The standards of moral conduct which seek to honor God
3. Student safety with regard to:
    a. safety on the Internet through avoidance of questionable activities and awareness that evil forces do lurk behind the anonymity provided by online presence;
    b. appropriate behavior while on online, on social networking Web sites, in chat rooms, and through email communications; and
    c. cyberbullying awareness and response.
4. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the School's acceptable use policies.

Adoption

This modified Internet Safety Policy was adopted by the Board of Rock County Christian School at a meeting of concerned stakeholders (board members, staff, parents/guardians), following normal public notice, on

August	31	2020
Month	Day	Year