Northside Christian School's Technology Acceptable Use Policy

Northside students and a parent (or legal guardian) are required to sign the Northside Christian School Acceptable Technology Use Agreement, available in the office. This agreement defines conditions of use of all computer technology, the computer network, phones, and other communication devices on school property, or during school activities. Failure to abide by the terms of this agreement may result in school discipline, termination of the use of the network, except for assignments requiring computer use, suspension from school, expulsion and/or reporting to legal authorities.

This document shall constitute Northside Christian School's Technology Acceptable Use Policy for students, staff, and other users. This policy applies to all users who access the network either on-site or remotely. A copy of this policy is available to students, their parents/guardians, and staff members.

Northside Christian School makes available to each student and staff member an interconnected computer system, computer equipment, computer programs, the Internet, email accounts, an Office 365 account, on-site or cloud data storage, and other technologies (collectively, "the network"). Northside Christian School filters the internet to block access to visual depictions deemed as obscene, pornographic, or harmful to minors. Any attempt to circumvent the filter is prohibited. The staff is committed to educating students in safe and appropriate online behavior, including but not limited to, e-mail, chat rooms, social media, and other forms of electronic communication.

Access to the school's network is provided as a privilege and as an educational tool. In order to continue enjoying access to the network, each user must take responsibility for appropriate and lawful use of this privilege. Students are responsible for their behavior on the network just as they are in a classroom, on school property, or at school activities.

Each user (students, staff members, and guests) is responsible for reading and abiding by this policy. Any questions about the provisions of this policy should be directed to the school administrator, technology director, or designee. Violations of this policy are considered violations of the Student Code of Conduct and may result in disciplinary action. Discipline could include access being limited or suspended by the school administrator, school suspension, expulsion, request for social media sites to remove content, and/or referral to law enforcement. The school reserves the right to seek reimbursement of expenses and/or damages arising from violations of these policies or reckless use of the equipment.

Families that have a more restrictive set of requirements for internet use should communicate those to their student.

<u>Staff, students, and other users shall comply with the following guidelines and procedures:</u>

<u>01. Reporting Misuse</u>

A user shall report any misuse of the network to a teacher, the technology director, or the school administrator. Misuse means any violation of this policy, such as commercial use of these

resources, criminal activity, inappropriate content of an e-mail sent or received, or any other use that is not included in this policy, but has the intent or effect of harming the school, another person, another's property, or that constitutes inappropriate conduct.

02. Term of the Permitted Use

Access to the network may be limited or suspended in compliance with Ohio law by the school administrator for violation of this policy. By accepting network access, users waive any and all rights of privacy in connection with their communications achieved through the use of school equipment, software, or connectivity.

03. Access

Network resources are for use only by authorized users, and access may not be shared or transferred. Users shall not share their passwords or otherwise allow anyone to gain unauthorized access to the network or the internet. Users are to notify the technology director, the school administrator or his/her designee immediately if they believe that someone may know their password. A user is subject to disciplinary action for any violations of this policy committed by someone else who, with the user's express or implied permission or through the user's negligence, accesses the network with the user's password.

04. Purpose and Use

The school is providing access to its network primarily to support and enhance educational experiences. Uses that interfere with normal school business, regardless of when or where they occur; or that violate school policies are strictly prohibited, as are uses for the purposes of engaging in or supporting any kind of business or other profit-making activity. Users shall consult with a teacher, school administrator, or technology director if there is any question of appropriate use.

05. Internet-based Accounts for Students

The school will assist students in setting up accounts on approved websites used as part of the curriculum and selected for their educational value. The website approval process will include a review by the technology director of the website's privacy policy to insure sufficient protection of the required personal information of the student in accordance with the Children's Online Privacy Protection Rule (COPPA).

06. Personal Devices

Use of personal devices is encouraged and permitted at school and school-related functions within certain bounds. Use of these devices is a privilege, which may be denied or forfeited by individual users if the guidelines are not followed. The user must submit, upon request, the identification characteristics (MAC address, IP address, device name, etc.) of any personally-owned device used within the school facility or at a school activity. Devices should be connected to the school's network unless not technically possible. Devices with video or photographic recording capability must not be used to capture any image in locations such as locker rooms or restrooms where any

student, staff member, or visitor may be changing clothes or be at any stage of disrobement. Use of the device must not disrupt or deter the educational process. Use of personal devices is not permitted in testing, examination, or assessment environments unless allowed by faculty or administration. The school assumes no responsibility in the case of damage to, or loss of, personal devices.

06. Unacceptable Uses

Other prohibited uses and activities include, but are not limited to the following:

A. Creating, copying, viewing, transmitting, downloading, uploading, or seeking sexually explicit, pornographic, obscene, violent, threatening, or other materials that would offend the school's standards.

B. Using, viewing, transmitting or downloading material containing inappropriate language, including swearing, vulgarities or other language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening. This includes using the network to make, distribute, or redistribute jokes, stories or other material that would violate this policy or the school's harassment, bullying, or discrimination policies – i.e., material that is based upon slurs or stereotypes relating to race, gender, disability, ethnicity, nationality, religion, sexual orientation, economic status, military status, political beliefs, or other protected personal or physical characteristics.

C. Engaging in harassment, stalking, or other repetitive unwanted communication, or using the internet in support of such activities.

D. Offering for sale or use or soliciting the purchase or provision of any substance the possession or use of which is prohibited by law or school policy.

E. Creating, copying, viewing, transmitting, downloading, or uploading any materials that include information for creating or obtaining an explosive device, dangerous ordinance, or any other materials useful in criminal activities or terrorist acts, or any other materials that violate or encourage others to violate the law or school policy.

F. Unauthorized copying, modifying, intruding, or attempts to copy, modify or intrude, into the folders, files, data, work, networks, passwords or computers of others, or intercepting and/or forwarding communications intended for others.

G. Copying, downloading, uploading or transmitting student information, images, pictures, or other confidential information outside of an official school activity and without school permission.

H. Transmitting or posting anything that reflects negatively on Northside Christian School or Calvary Bible Church.

I. Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. The school intends to strictly abide by the Copyright Laws of the United States. Any materials used that are covered by Copyright shall be used by permission or through "fair use" or other allowable methods created by the Copyright Act.

J. Soliciting political contributions through the network from any person or entity or conducting any type of political campaign.

K. Hacking, altering, harming, destroying or interfering with the normal operation of software, hardware, data of another user, other network resources, or the use of the network to do any of the same acts on the internet or outside networks. This includes any attempt to go around school filters and other protection devices.

L. Vandalism, creating viruses, malicious attempt to harm or destroy equipment or data or materials of any other user; degrading or disrupting the operation of the network.

M. Recreational web browsing or engaging in other activities that waste computer, paper, or telephone resources; or that cause unnecessary traffic, however harmless the activities may seem to be.

N. Installing or downloading software or hardware. Students may not attempt to repair, reconfigure, or modify network equipment, computers or systems. Students shall not remove, alter, or copy school software for their own personal use or for the use of others. Only the technology director or his/her designee may install hardware or software.

O. Supporting any kind of business or other profit-making activity. Students may not sell or buy anything over the internet, nor solicit or advertise the sale of any goods or services.

P. Violating the standards of academic or personal integrity, including but not limited to plagiarism, disseminating untrue information about individuals or groups, or maliciously hiding one's true identity.

Q. Using telephones, electrical communication devices, or other electronic devices on school property or at a school-sponsored activity to access and/or view internet web sites that are otherwise blocked to students at school.

R. Users, except staff members in the conduct of official school business, may not provide any personal information about themselves or anyone else using the school's network or issued email.

S. Use of e-mail or social network sites to defame, harass, intimidate, or provoke anyone.

07. Freedom of Speech

By giving users access to this system, the school does not intend to create a limited or a public forum for the expression of opinion. The network exists as part of the mission of Calvary Bible Church and Northside Christian School, and is operated solely in support of that mission. Neither the guests, staff, nor students are invited to use the school's network in expression of their opinion.

Updated 1/1/19