DES MOINES CHRISTIAN SCHOOL
ACCEPTABLE USE OF TECHNOLOGY

This Policy sets forth basic guidelines that all students and employees of the District are expected to follow when using any District-owned network or device (as defined below).

The district is not responsible for systems or networks over which it has no control. Parents and/or guardians of minors are responsible for setting and conveying the standards that their children should follow when using these electronic resources and online environments at home. Failure to abide by District policy and administrative regulations governing the use of these resources may result in the suspension and/or revocation of system access. Additionally, any student violation may result in discipline up to and including expulsion. Staff violations may also result in discipline up to and including dismissal.

All users must sign the Acceptable Use Policy Agreement before accessing any DMCS technology resource.

DISTRICT OWNERSHIP

The District, at its sole discretion, may provide access to various technological resources, including but not limited to the Internet and the District's network, District email, web resources and platforms, computing devices (including desktop computers, laptop computers, and tablets and all peripheral devices thereto) to employees and students. The District may also, at its sole discretion, provide employees with access to District voicemail, cell phones, and/or smart phones as necessary to perform their job duties. Collectively, these resources will be referred to as the District's "Network Resources."

The District provides these Network Resources as a benefit to students and employees for the sole purpose of enhancing the educational opportunities offered by the District.

Use of all DMCS Network Resources is a privilege and not a right.

NO EXPECTATION OF PRIVACY

All of the District's Network Resources are District property and are not confidential.

The District has the right to access, review, copy, modify, and delete any information transmitted through or stored in the District's systems or devices, including but not limited to e-mail, web postings, text messages, and other electronic communications.

Files containing personal information about a student or employee that are transmitted through or stored in the District's systems or devices are treated no differently that the District's other files, and students and employees have no expectation of privacy in such. All communications sent over the DMCS network or to or from any DMCS-provided account or device, including text and images, may be subject to disclosure to

applicable law enforcement or other third parties without prior consent of the sender or the receiver, as provided by law.

USER'S RESPONSIBILITY

Users shall be responsible for the proper use of all DMCS Network Resources issued or made available to them by the District. Students are responsible for immediately notifying a staff member of any damage to the device that they are using. Employees must immediately report any damage to District-issued devices to the IT Manager.

NETWORK SECURITY AND SAFETY

To the extent required by federal law, the District shall use technology protection measures to protect against the access of inappropriate materials online.

The District will monitor the online activities of students and will provide age-appropriate education and training about the provisions of this policy, including safe and appropriate online behavior (including interaction on social networking sites and chat rooms) and cyber bullying awareness and response.

All users must follow these guidelines for promoting network security and safety:

- Users shall not share their accounts with anyone or leave the account open or unattended.
- Passwords shall remain confidential and should be protected by the user and not shared or displayed.
- Users are responsible for immediately contacting District IT staff or administration of any possible security problems.
- For personal safety reasons, users should never reveal their full name, address or location, telephone number, or any other personally identifiable information using District Network Resources. Students should only communicate with others online using District Network Resources for educational purposes. Students should never share personally identifiable information or arrange a meeting in person with an individual whom they met online.
- Users should immediately inform a staff member or administrator of any online communication that is threatening, harassing, or otherwise inappropriate.

ACCEPTABLE USES OF TECHNOLOGY

Responsible Use

A. The authority for monitoring acceptable use of electronic Internet resources is delegated to DMCS District staff members assigned to classrooms and the technology department.

B. Instruction in the proper use of the Internet will be provided to staff members who will then provide similar

instruction to students.

C. Students and staff members are expected to practice appropriate use of the Internet, including compliance with applicable laws and District policies.

Violations may result in disciplinary action.

D. The smooth operation of the network relies upon the proper conduct of the users who must adhere to strict guidelines that require efficient, ethical and legal utilization of the computer network.

E. Users are responsible for the content of all text, audio or images that they place on or send over the Internet.

F. If a student gains access to any service via the Internet, which has a cost involved, or if a student incurs other types of costs, the student accessing such a service will be responsible for those costs.

G. Any use of the Internet, technology, or transmission of material, information or software in violation of any federal, state, or local law or regulation, board policy, or building regulation is prohibited.

Online Etiquette

A. Users are expected to learn and abide by generally accepted rules of Internet network etiquette as well as school board policy regarding student conduct.

B. Students should use common courtesy, politeness and should avoid vulgar language, sarcasm, insults, and humor. Without face-to-face contact, comments can easily be misconstrued as criticism.

C. Apply the same privacy, ethical and educational considerations that are utilized in other forms of communication.

D. Each web site may have its own set of policies and procedures. It is the user's responsibility to abide by those policies and procedures.

E. Respect all copyright and license agreements.

F. Cite all quotes, references and sources taken from web sites.

Rules Applicable to Specific Network Resources

Internet

A. The Internet may be used by students and staff for school appropriate research for reference, or other legitimate educational purposes.

B. Users should attempt to access only school-appropriate material when using search engines such as

Google, Bing, etc. to find websites, images, or files.

C. Users should only use social networking sites or other interactive web platforms for classroom courses or content.

D. Should users encounter inappropriate material by accident, they should leave the site immediately.

E-Mail

All users of email accounts, regardless of whether or not they are school-issued or personal, must adhere to the following guidelines:

A. Use of objectionable language is prohibited.

B. Always sign messages.

C. Always use caution when addressing messages to ensure that messages are not inadvertently sent to the wrong party.

D. Acknowledge receipt of a document or file when appropriate.

E. Transmission, creation, or access of bullying or harassing, defamatory, obscene, pornographic, profane, offensive, threatening, or discriminatory messages or messages that disclose personal or confidential information without authorization is strictly prohibited.

F. Use of the DMCS Network or DMCS-provided accounts or devices to improperly distribute copyrighted materials is prohibited.

G. Passwords must be kept in a discreet location and shall not be shared with anyone. Any employee identified as a security risk or having a history of problems with information security may be denied access to the DMCS Network and DMCS-provided accounts and/or devices.

H. Use of another's user name/account to access e-mail or the Internet, with or without that user's permission, is strictly prohibited.

Computers, Laptops, Tablets, and Other Similar Devices

A. Users should log in using their username when possible. Use of another's username and password, with or without that user's permission, is strictly prohibited.

B. Users who log into a public username should be aware that any documents left on the desktop or in the documents folder could be seen by other users using the same public username, and may be deleted at any time. Users should remove any personal documents on the desktop or in the documents folder before logging out.

C. Users will handle all physical components of the computing or communication device, including all peripherals with care while using a computer. Keyboards and mice should be kept with computer workstations and not moved. Mobile devices (laptops, iPads, etc.) must be properly stored and plugged in (as appropriate) when not in use.

Digital Storage Devices

A. Users are responsible for ensuring any data stored on such a device is virus-free and should only be used to store the owner's school appropriate material.

Cell Phones, Smart Phones, and Other Handheld Devices

A. Student use of cell phones is regulated by each principal. Permission for use of all other handheld devices must be obtained from a staff member for students to use them.

B. Students may only use cell phones, smart phones, or other handheld devices with staff permission in accordance with to each department's policy.

PERIPHERAL DEVICES

A. Students will use peripherals under the direction and/or permission of staff.

B. Users should print only when necessary and in quantities necessary and are responsible for any costs associated.

UNACCEPTABLE USES OF TECHNOLOGY

The District strictly prohibits inappropriate uses of the Internet and District Network Resources, including e-mail, web postings, text messages, and other online communications, which include but are not limited to the following:

A. Disclosure of confidential or sensitive information known or entrusted to the District to any unauthorized individual.

B. Misuse of copyrighted material or other copyright violations.

C. Communicating in ways that disparage others.

D. Communicating information that could be perceived as an official District position or endorsement without prior approval by proper District officials.

E. Using confrontational or improper language or making defamatory statements.

F. Creating, storing, viewing, or transmitting defamatory, pornographic, obscene, profane, illegal, or otherwise offensive material. If a user encounters such prohibited material, the user should immediately terminate contact with the material and notify appropriate District personnel.

G. Participating in any activity that could be interpreted as bullying, harassment, or discrimination.

H. Misrepresenting an individual's identity or the source of communications or data.

I. Attempting to break into any other Internet server, network, file, or similar device.

J. Accessing confidential information on District Network Resources without permission.

K. Promoting political or religious positions (including violations of ethics and campaign disclosure laws).

L. Participating or engaging in activities that violate any local, state, federal, or international law, or any District policy, rule or standard.

M. Operating a personal business or using District Network Resources for personal

N. Exporting or importing of any governmentally controlled technical data (such as software encryption) to or from authorized locations or persons, without appropriate licenses or permits.

O. Disrupting the use of the District's Network by other users, or wasting system resources.

P. Sending unsolicited messages (including spam).

Q. Vandalizing District Network Resources through any malicious act or the attempt to harm, modify, or destroy the computer property or data of the District or another user, the Internet, or District Network Resources, or any other technologies or devices used in the District. This includes but is not limited to causing physical damage to devices as well as participation in hacking or the uploading or creation of viruses or other malicious programs to any District Network Resource.

HARASSMENT AND BULLYING

In accordance with Iowa law, the District's policy prohibiting bullying and harassment applies to all electronic communications. Employees and students are prohibited from engaging in any bullying or harassing behavior via any electronic means, including those means that are not part of the District's Network Resources.

VIOLATIONS AND SANCTIONS

All users are expected to abide by the provisions of this Policy. Any student who uses technology in an

unacceptable manner is in violation of the district's Student Behavior and Discipline Policy and will be subject to sanctions as stated in the policy. Since the nature of each violation may vary, the supervising classroom teacher and/or building administration is given broad discretion in determining the severity of the sanction.

Students will be given written notification of the violation and sanction as stated on the Technology Acceptable Use Violation Notice.

Technology Acceptable Use Violation Notice

Staff members who use technology in an unacceptable manner may also be subject to disciplinary actions up to and including dismissal.

Violations of this Policy may also result in the loss of a user's privileges to use any or all District Network Resources for an appropriate period of time to be determined by the supervising classroom teacher and/or administrator. Sufficiently severe violations may result in permanent loss of privileges, as determined by a principal.

District administration may confiscate any District-owned device from a student or employee, due to violation of this policy.

The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District will not be responsible for any damages that employees or other persons may suffer. This includes damages due to loss of data resulting from delays, no deliveries, mis-deliveries, or service interruptions, whether caused by the District's own negligence or the employee's errors or omissions.

The District specifically denies any responsibility for the accuracy or quality of information obtained through its Services.

Student Internet User Agreement Parent / Guardian Permission Form

One form per Student

As a parent or legal guardian of the student listed below, I have read the DMCS Acceptable Use Policy and grant permission for my daughter or son to access networked computer services and the Internet. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use, setting and conveying standards for my daughter/son to follow when selecting, sharing, or exploring information.

Student Name (please print)

Parent / Guardian Signature

As a user of the DMCS computer network, I have read and hereby agree to comply with the stated rules, communicating over the network in a responsible fashion while honoring all relevant laws, school rules, and restrictions.

Student Signature:

Date: _____ Grade: _____