Christ Community Lutheran School

Acceptable Use Policy
for using technology at CCLS

Philosophy for the Use of Technology
We believe that technology is a tool for communication, for problem solving, and for academic achievement. Technology does not end with itself, but is used by students, parents, staff, and the entire school community to access information in the school, the community, and the world. Technology tools are used by students to learn grade level and course content based on Christ Community Lutheran School adopted curriculum standards. As in the real world, students use technology to work on challenging, real-life topics, to present their conclusions to important questions, and to defend and clarify their thinking. All technology tools are used in support of the vision of Christ Community Lutheran School to minister to real people in a real way.

Technology at Christ Community Lutheran School
CCLS aims to be at the forefront of technological development. Interactive whiteboards (SMART Boards) and digital projectors are in every classroom. Senteo responders and Airliners are used to several classrooms. CCLS maintains mobile laptop carts with Chromebooks at the elementary school for grades 3 and 4. A mobile iPad cart is available for K – 2 to be used in classroom centers or in a 1:1 environment in the classroom. Grades 5 and 6 have 1:1 Chromebooks for use during the school day. Our 7th and 8th grade students receive iPads for their technology tool. CCLS has upgraded the network infrastructure to support a wireless network for WiFi. CCLS will continue to move to the cloud with Google.

Internet Acceptable Use Policy
Christ Community Lutheran School believes the internet is a resource that the school and students should positively utilize. There is no simple technological solution to the problem of keeping children safe online. One factor in internet safety is to ensure appropriate supervision. The CCLS staff is aware of the issues surrounding internet access and the need for appropriate supervision. CCLS will filter internet content using Open DNS. The school cannot control internet access by pupils using their own devices with separate internet access (for example, smart phones). However, the school does regard any access of inappropriate material on school property or during school hours to be a disciplinary matter. Parents have the responsibility to be aware that there may be risks associated with Internet access and the steps the school is taking to address these issues. Parents will also wish to ensure safe use of the Internet in the home. Following are wise guidelines for students using the internet no matter the location:

- Let your online behavior be an example for others, and reflect the values and beliefs we share as followers of Jesus.

> [8]*Finally, brothers, whatever is true, whatever is noble, whatever is right, whatever is pure, whatever is lovely, whatever is admirable—if anything is excellent or praiseworthy—think about such things.* [9]*Whatever you have learned or received or heard from me, or seen in me—put it into practice. And the God of peace will be with you. (Phil 4:8-9) (NIV)*

- Respect the rights and property of others.
  - If you use someone else's writing, video, images, or sounds be sure to get permission and/or give them credit.
  - Don't log on to someone else's account, even if they give you permission. Watch out for the safety of others.
  - If you discover someone else's password, let them know and encourage them to change it.

- Never pretend to be someone else while online.
- When communicating online using instant message (IM), e-mail, discussion boards, chat, or text message, remember to always be respectful. Use your words to build others up. Do not be mean, or hurtful.

- Protect yourself. Not everyone online shares your values and beliefs. There are people out there looking to take advantage of you or maybe even harm you, so protect yourself while online.

  - Protect your passwords. Do not share them with others.
  - When you are posting something that could be viewed publicly, never give out any personal information that could let someone you don't know be able to find you.
  - If inappropriate material should appear on your computer screen, tell an adult immediately.
  - If someone sends you inappropriate material, tell an adult immediately.
  - Do not communicate with a stranger. If you are contacted by an unfamiliar user, tell an adult immediately.

CCLS Network

Students and staff may use the school network for educational purposes. Access to the network is a privilege that may be revoked at any time for inappropriate conduct. Users of Christ Community Lutheran School should have no expectation of privacy when using our technological resources.

Email

- Only the approved mail service given by Christ Community Lutheran School may be used for student mail.
- The school reserves the right to search and read email as deemed necessary.
- Email during class is prohibited unless authorized by faculty or administration.
- Students should always use appropriate language in their email.
- Email services provided by the school are to be used only for the exchange of appropriate information.
- No inappropriate email is allowed including derogatory, obscene, or harassing messages. Email messages of an abusive or harassing nature will be subject to a disciplinary response.
- Chain letters of any kind and spam are prohibited. Chain letters are defined as any email message asking you to pass information or messages on to other individuals or groups via e-mail.
- Students are prohibited from accessing anyone else's email account without first receiving explicit permission from the account holder.
- Email etiquette should be observed. In general, only messages that one would say to the recipient in person should be written.
- School email addresses are not to be given to ANY websites, companies, or other third parties without the explicit permission of a teacher or administrator.

Instant messaging

- Instant messaging (e.g., iChat, aim, gTalk, skype, Facetime) is prohibited on campus except as part of an assigned, in-class activity that is supervised by faculty or administration.
- Participation in chat rooms during school hours is prohibited, except as part of an assigned, in-class activity.

Audio and Video

- Audio on computers should be turned off unless required for the activity being conducted.
- Listening to music either aloud or with earphones is not permitted during class, without the permission of the teacher.
- The use of laptops to watch movies and DVD videos is not permitted during the school day.
- Any audio or video recording may be conducted only with prior permission of all parties being recorded.
- Sharing of music (including iTunes music sharing) over the school network is strictly prohibited.

Games

- Games are not permitted during school hours except as part of an assigned, in-class activity.
- The school reserves the right to remove any game from a school computer.
- Screen savers that include gaming components are not allowed.

iPads & Chromebooks

- Student iPads and Chromebooks must not be left unattended at any time. If a mobile device is found to be unattended, it will be turned in to the school office.
- iPad and Chromebooks must be in a student's possession, secured in a locked classroom or computer cart at all times.
- iPads and Chromebooks must be carried and transported appropriately. Chromebooks should be closed and carefully carried.
- No food or beverages should be in the vicinity of the iPads and Chromebooks. iPads and Chromebooks may not be used in the dining hall during lunch.
- iPads and Chromebooks should be handled with respect and care. Inappropriate treatment of iPads and Chromebooks is not acceptable.

Network Access

- Students must not make any attempt to access servers or network information that is not open to the public.
- The utilization of proxy avoidance IP numbers and programs is strictly prohibited.
- Students may not use the school network for personal or private business reasons.
- Students are not to knowingly degrade or disrupt online services or equipment as such activity is considered a crime under state and federal law. This includes tampering with computer hardware or software, vandalizing data, invoking computer viruses, attempting to gain access to restricted or unauthorized network services, or violating copyright laws.
- Students may not download large files which tax the ability of the school's network to operate efficiently or any other applications that cause serious congestion on the campus network and interfere with the work of others.
- Students may not tamper with network cabling or routing devices installed on campus.

File Sharing

- File sharing is the public or private sharing of computer data or space. Any program that creates a point–to–point connection between two or more computing devices for the purpose of sharing data is considered file sharing.
- File sharing of any kind is prohibited both on campus and off campus. The only exception to this is when it is a specific assignment given by a faculty member.
- No file sharing software of any kind is to be installed on school computers including laptops. Examples of this type of software are Limewire, Bearshare, Kazaa, uTorrent, etc. Although these types of programs are software downloads, they automatically create file sharing connections.

Downloading and Loading of Software

- The downloading of music files, video files etc. through the school's network is prohibited unless it is part of an assigned, in-class activity.
- Copyrighted movies may not be "ripped" from DVD's nor may copyrighted movies be downloaded from the internet to CCLS technology devices. Only commercial videos legally purchased from the iTunes music store or another like entity may be downloaded.

Shareware and Freeware

- Shareware and freeware programs such as animated cursors (i.e., Comet Cursor), screen savers, and others are prohibited. Software like these automatically open connections to the computers from the outside of our network. Those connections are spyware, and they not only monitor the activities on that computer, but they also slow down the operation of the computer and the network connection.

Internet Use

- The Internet is a rich and valuable source of information for education. Inappropriate materials are available on the Internet, but are strictly prohibited. These materials include items of a sexual or pornographic nature, extremist or militant materials, gambling, depictions of violence, images that are intended to be abusive or harassing, etc. Students must not access, display, or store this type of material.
- Information obtained through the Internet must be properly cited and in compliance with copyright laws.

- Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- Plagiarism includes the use of any information obtained from the Internet that is not properly cited. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism.
- If a student accidentally accesses a website that contains obscene, pornographic or otherwise offensive material, it is the responsibility of the student to notify a teacher as quickly as possible so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.

Privacy, Use, and Safety

- Students may not give any personal information regarding themselves or others through e-mail or the Internet including name, phone number, address, passwords, etc. unless they are completely sure of the identity of the person with whom they are communicating. Frequently the identity of someone on the Internet is impossible to confirm; therefore contact with such individuals is considered inappropriate and unsafe.
- Students must secure and maintain private passwords for network/laptop and e-mail use. This is important in order to protect the privacy of each student.
- The school administration has the right to view any files in order to investigate suspected inappropriate behavior.
- The school will monitor computer activities that take place on campus during the school day including logging website access, newsgroup access, bandwidth, and network use.
- Students are prohibited from accessing faculty, administration, and staff computers as well as school file servers for any reason.
- Students are prohibited from utilizing the command prompt interface. In addition to this, students are prohibited from using any method to obtain control of another person's computer through the use of their own computer.
- Students are prohibited from using laptops or any computer for acts of cruelty (including mean-spirited e-mails, offensive blogging, cyberbullying etc.).

Use of WiFi Network

Pupils may access the school Wifi network on devices managed by the school.

Mobile Devices

Students found accessing inappropriate material on their own mobile devices such as a mobile phone , iPad, Kindle, etc. may have these removed from their possession for the duration of the school day and may be banned from having them in school. Additional formal action may also be taken as is appropriate.

Cameras

Students should not use cameras (including cameras built into mobile devices) in school without the permission of a teacher. Under no circumstances should cameras be used on the playground, in restrooms, or in other private places.

Social Networking

This section of the policy refers to the use of social media sites such as, but not limited to Facebook, Twitter, YouTube, etc. Teachers and students may not mention members of the school community without their consent unless the subject is of public concern and the speech falls under the applicable constitutional protections.

Copyright

Unauthorized duplication, installation, alteration, or destruction of data programs, hardware, or software is prohibited. Data, programs, hardware, software, and other materials including those protected by copyright may not be transmitted or duplicated.

Consequences

The school reserves the right to enforce appropriate consequences for the violation of any section of the Acceptable Use Policy. Any violation of Christ Community Lutheran School's Acceptable Use Policy may result in loss of school provided access to electronic information. Consequences will be applied to student misuse of school property, including, but not

limited to, the loss of the use of the technology device for an amount of time determined by the administration and the technology department, disciplinary action including suspension and referral for expulsion, and possible legal action. Students with computers or mobile devices containing illegal or inappropriate materials may be subject to having content removed from the device and may be subject to more frequent random checks, and may be subject to having the device re-imaged.* These students may face possible fines because of damage or labor charges.

**Christ Community Lutheran School is not financially responsible for any student purchased content lost during the re-imaging process. In the case of repeated iPad or Chromebook abuse and/or damages, the school has the right to revoke the use of the school's technology device. Repeated AUP offenses or laptop abuses may lead to the loss of student privilege to use a laptop or other technology devices on campus. Additional action may be determined by the executive director and principals. Illegal actions are subject to prosecution by local, state, or federal authorities. Christ Community Lutheran School takes no responsibility for activities conducted on school computers or materials stored on computers, laptops, Chromebooks, iPads or the school's network.*

National Technology Standards for Students (NETS-S)

Standards for Grades K-12

1. Creativity and Innovation. Students demonstrate creative thinking, construct knowledge, and develop innovative products and processes using technology.
2. Communication and Collaboration. Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others.
3. Research and Information Fluency. Students apply digital tools to gather, evaluate, and use information.
4. Critical Thinking, Problem Solving, and Decision Making. Students use critical thinking skills to plan and conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools and resources.
5. Digital Citizenship. Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.
6. Technology Operations and Concepts. Students demonstrate a sound understanding of technology concepts, systems, and operations.

The profiles below highlight a few important types of learning activities in which students might engage as the new NETS-S are implemented. These examples are provided in an effort to bring the standards to life and demonstrate the variety of activities possible. The numbers in the parentheses after each item identify the standards (1-6) most closely linked to the activity described. Each activity may relate to one indicator, to multiple indicators, or to the overall standards referenced.

Profiles for Grades K-2

The following experiences with technology and digital resources are examples of learning activities in which students might engage during PK-Grade 2 (Ages 4-8):

1. Illustrate and communicate original ideas and stories using digital tools and media-rich resources. (1,2)
2. Identify, research, and collect data on an environmental issue using digital resources and propose a developmentally appropriate solution. (1,3,4)
3. Engage in learning activities with learners from multiple cultures through e-mail and other electronic means. (2,6)
4. In a collaborative work group, use a variety of technologies to produce a digital presentation or product in a curriculum area. (1,2,6)
5. Find and evaluate information related to a current or historical person or event using digital resources. (3)
6. Use simulations and graphical organizers to explore and depict patterns of growth such as the life cycles of plants and animals. (1,3,4)
7. Demonstrate safe and cooperative use of technology. (5)
8. Independently apply digital tools and resources to address a variety of tasks and problems. (4,6)
9. Communicate about technology using developmentally appropriate and accurate terminology. (6)
10. Demonstrate the ability to navigate in virtual environments such as electronic books, simulation software, and Web sites. (6)

Profiles for Grades 3-5
The following experiences with technology and digital resources are examples of learning activities in which students might engage during Grades 3-5 (Ages 8-11):

1. Produce a media-rich digital story about a significant local event based on first-person interviews. (1,2,3,4)
2. Use digital-imaging technology to modify or create works of art for use in a digital presentation. (1,2,6)
3. Recognize bias in digital resources while researching an environmental issue with guidance from the teacher. (3,4)
4. Select and apply digital tools to collect, organize, and analyze data to evaluate theories or test hypotheses. (3,4,6)
5. Identify and investigate a global issue and generate possible solutions using digital tools and resources (3,4)
6. Conduct science experiments using digital instruments and measurement devices. (4,6)
7. Conceptualize, guide, and manage individual or group learning projects using digital planning tools with teacher support. (4,6)
8. Practice injury prevention by applying a variety of ergonomic strategies when using technology. (5)
9. Debate the effect of existing and emerging technologies on individuals, society, and the global community. (5,6)
10. Apply previous knowledge of digital technology operations to analyze and solve current hardware and software problems. (4,6)

Profiles for Grades 6-8
The following experiences with technology and digital resources are examples of learning activities in which students might engage during Grades 6-8 (Ages 11-14):

1. Describe and illustrate a content-related concept or process using a model, simulation, or concept-mapping software. (1,2)
2. Create original animations or videos documenting school, community, or local events. (1,2,6)
3. Gather data, examine patterns, and apply information for decision making using digital tools and resources. (1,4)
4. Participate in a cooperative learning project in an online learning community. (2)
5. Evaluate digital resources to determine the credibility of the author and publisher and the timeliness and accuracy of the content. (3)
6. Employ data-collection technology such as probes, handheld devices, and geographic mapping systems to gather, view, analyze, and report results for content-related problems. (3,4,6)
7. Select and use the appropriate tools and digital resources to accomplish a variety of tasks and to solve problems. (3,4,6)
8. Use collaborative electronic authoring tools to explore common curriculum content from multicultural perspectives with other learners. (2,3,4,5)
9. Integrate a variety of file types to create and illustrate a document or presentation. (1,6)
10. Independently develop and apply strategies for identifying and solving routine hardware and software problems. (4,6)

Students are required to adhere to all provisions and conditions set forth in this Acceptable Use Policy. Students are to report any known violations of this Acceptable Use Policy to appropriate administrative staff members. Christ Community Lutheran School reserves the right to make changes or additions to the acceptable use policy. The most current edition is always available at www.ccls-stlouis.org.

Acceptable Use Policy

for using technology at CCLS

By signing here, I am acknowledging that I have read, understand, and agree to follow the policies as stated in the Acceptable Use Policy for using technology at CCLS, both at school and away from school. I understand that my bad choices could lead to consequences as outlined in this policy and the school handbook.

_____ _____

student signature *date* *parent signature* *date*