

St. Cecilia Catholic School
Borrowed Device Care & Acceptable Use Policy (BDAUP)

Dear Parents:

Your child has the opportunity to access technology resources at ***St. Cecilia Catholic School***. With this educational opportunity also comes responsibility. It is important that you and your child read the enclosed Borrowed Device Care and Acceptable Use Policy (BDAUP) and Permission Form and discuss it together.

When your child is given an account and password to use on the computer, it is extremely important that the rules and policies be followed. Failure to follow the rules will result in the loss of the privilege to use this educational tool.

Remember that you are legally responsible for your child's actions. Please stress to your child the importance of using only his or her own account and password, and the importance of keeping it a secret from other students. Under NO circumstances should your child let anyone else use his or her account and password. Please refer to your school's parent/student handbook for policies regarding cell phones/Iphones, and any other mobile devices.

Although we have established acceptable use policies, please be aware that there may be unacceptable material or communication on the Internet that your child can access. Attention and appropriate supervision should be exercised.

Personal care of the device is paramount. Please talk to your child about storage, transportation, and the possibility of device breakage. Regardless of the cause, breakages that require repair will be charged for repairs: \$50 for the first instance, \$100 for the second instance, and \$150 for the third instance. For negligent or total loss, the replacement cost is \$350. These fees will be assessed through FACTS, as needed.

After you have read and discussed this with your child, please check the appropriate boxes, have both you and your child/children sign the agreement, and return it to the school office.

In Him we trust,

Jeff Matthews, Principal

St. Cecilia Catholic School

Borrowed Device Care & Acceptable Use Policy (BDAUP)

Borrowed Device Acceptable Use Policy

With the use of technology, including the Internet, virtual network, hardware, and software, St. Cecilia Catholic School is expanding learning access for students, staff, and parents. With this opportunity comes the responsibility for appropriate use.

Electronic Network Use Guidelines

The operation of technology relies heavily on the proper conduct of the users. Every St. Cecilia Catholic School user has the responsibility to respect and protect the rights of every other user in our community. St. Cecilia Catholic School users are expected to act in a responsible, ethical and legal manner, in accordance with the missions and purposes of the networks they use on the Internet and with the laws of Texas and the United States.

School computer systems are for use by authorized individuals only. Any unauthorized access to these systems is prohibited and is subject to criminal and civil penalties. Use of any other network or computing resources must be consistent with the rules appropriate to that network. All network users are expected to use moral and ethical guidelines in making appropriate decisions regarding network use.

Use of the district network is not a right, but a privilege, and inappropriate use will result in cancellation of that privilege, disciplinary action, and/or prosecution. Prior to participation, a potential network user will receive information pertaining to the proper use of the network and sign a user agreement. School and district administrators will decide what constitutes inappropriate use of the network and their decision is final. Violations will be dealt with in accordance with the St. Cecilia Catholic School Student Code of Conduct policy or employee handbook code of conduct, or local, state or federal law.

This unacceptable conduct includes, but is not limited to:

- Using the network for any illegal activity
- Transmitting material in violation of any federal, state, or local law or school district policy
- Violating software copyright or other contracts
- Using school technology for financial or commercial or personal gain
- Degrading or disrupting equipment or system performance
- Vandalizing hardware
- Vandalizing the data of another user
- Wastefully using finite resources

- Unauthorized use of school resources, including hardware (ie. Digital camera, projector, etc.) and printers for reasons other than school assignments and activities
- Gaining unauthorized access to resources or entities
- Invading the privacy of individuals
- Using someone else's username and password
- Placing of unlawful information on a system
- Using for political lobbying
- Intentionally accessing pornographic, inappropriate or unauthorized material either directly or by proxy
- Intentionally bypassing school network security and firewall systems and/or policies
- Intentionally transmitting viruses that may result in the loss of recipients' work or systems
- Chain letters or any type of use that would cause congestion of the networks or otherwise interfere with the work of others
- Installing software onto computers without appropriate approval.

Warranties

St. Cecilia Catholic School and joint providers of the network make no warranties of any kind, whether expressed or implied, for the services provided. St. Cecilia Catholic School will not be responsible for any damages suffered while using the system. These damages include, but are not limited to, loss of data, delays, non-deliveries, service interruptions caused by the system, or service interruptions caused by errors or omissions of the user. St. Cecilia Catholic School specifically disclaims responsibility for the accuracy or quality of information obtained through Internet connections.

Security

Security is a high priority due to the number of users. Computer security cannot be made perfect, and it is likely that a determined user could access computer resources for inappropriate purposes or that an inquisitive user could encounter unacceptable material. Identified security problems should be reported to a system administrator or appropriate teacher immediately and not shared with other users. Attempts to log on as another user may result in cancellation of user privileges. Any user identified as a security risk will be denied access to the system.

Vandalism

Vandalism is defined as any deliberate attempt to harm or destroy data or property of another user or St. Cecilia Catholic School, the Internet/Intranet, or other networks. This includes the creation of or the uploading of computer viruses to the Internet/Intranet or host site and destruction of hardware. Vandalism will result in cancellation of user privileges.

Harassment

Harassment is defined as targeting another person, group or organization to cause distress, embarrassment, injury, unwanted attention or other substantial discomfort. Personal attacks or other actions to threaten, intimidate or embarrass an individual, group or organization are prohibited. Users of the St. Cecilia Catholic School Network are expected to respect the rights of others to have freedom from harassment or intimidation.

Installing Apps, Add-ons, & Extensions

Use of computer software is governed by copyright laws and network configurations. Care must be taken to avoid copyright violations and disruptions of the network related to incompatible or corrupted software; therefore, installation of any program or application onto any computer with access to the St. Cecilia Catholic School electronic network must be approved by the Technology Coordinator, the Assistant Principal, or the Principal. Apps, add-ons, extensions will be increasingly managed through the St. Cecilia Chrome Web Store.

Monitoring

The information networks are "public places" and user actions are visible to others on the network. St. Cecilia Catholic School has the right to monitor network use to ensure that the network continues to function properly for all of its users. Anyone using electronic networks expressly consents to such monitoring. Monthly reports of Internet use are generated and shared with campus administrators, and usage is monitored through firewalls and the *GoGuardian* application. Prosecution and/or termination of user privileges can occur without warning. Usage may be monitored at home when logged into Chrome accounts.

Network Safety Policy

It shall be the responsibility of all St. Cecilia Catholic 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 Protecting Children in the 21st Century Act.

Use of Internet and other telecommunication activities must be in support of education and research that is consistent with the educational goals, objectives, and policies of St. Cecilia Catholic School.

All network users are expected to use moral and ethical guidelines in making appropriate decisions regarding Internet use. Use of the Internet is not a right, but a privilege, and inappropriate use will result in cancellation of that privilege. Prior to participation, a student will receive information pertaining to the proper use of the Internet and sign a user agreement.

School and district administrators will decide what constitutes inappropriate use of the Internet direct electronic communications. Their decision is final.

In the classroom, student access to and use of the Internet will be under teacher direction and will be monitored as any other classroom activity; however, it is impossible to control all materials on a global network and users may encounter inappropriate information. Even with filtering St. Cecilia Catholic School cannot prevent the possibility that some users may access material that is not consistent with the educational mission, goals and policies of the school.

School servers that provide Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or to any material deemed harmful to minors as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

With access to computers and people all over the world, there may be some material or individual communications which are not suitable for school-age children. St. Cecilia Catholic School views information gathered from the Internet in the same manner as other reference materials identified by the schools. Specifically, the school supports resources that will enhance the learning environment with directed guidance from the faculty and staff.

Publishing

The school respects the rights of parents to restrict their children from publishing on the Internet and will secure parent permission for the current school year. Parents will be required to sign a form if they choose to deny having student work, pictures, and/or student's name appears on the Internet/Intranet. When publishing student work, student first names and last initial will be used to identify student work, if at all.

Distance Learning

Students may have the opportunity to participate in distance learning activities including virtual field trip connections with entities such as zoos, museums, universities, and government agencies. Classes may also participate in point-to-point connections with other classrooms around the world or multi-point conferences connecting many classrooms. In a distance learning environment, the teacher and students' voice, physical presence and participation in classroom activities will be transmitted to other distance learning sites. These events may or may not be recorded.

Digital Citizenship

Digital citizenship can be defined as the norms of appropriate, responsible behavior with regard to technology use. It will be expected that all students/faculty/staff that has access to a Chromebook follow and adhere to these guidelines.

1. Looking after yourself by:

- Choosing online names that are suitable and respectful.
- Only inviting people you actually know in the real world to be your friends in the online world.
- Only visiting sites that are appropriate and respecting the rules that websites have about age. Some sites are only for adults. If you wouldn't feel comfortable showing the website to you parents or grandparents then it's inappropriate.
- Setting your privacy settings so that only the people you know can see you and your personal information.
- Using passwords that are hard to guess and keep these secret.
- Only putting information online that is appropriate and posting pictures that are suitable. Not everyone seeing your profile or pictures will be friendly.
- Always reporting anything that happens online which makes you feel uncomfortable or unhappy.
- Talking to trusted adults, like your parents and teachers, about your online experiences. This includes both the good and the bad experiences.

2. Looking after others:

- Show you care by not triggering (sending hurtful or inflammatory messages) other people, or forwarding messages that are unkind or inappropriate.
- By not getting involved in conversations that are unkind, mean or bullying.
- By reporting any conversations you see that are unkind, mean or bullying. Imagine if the things being written were about you. If you would find them offensive then they are inappropriate.
- Some websites are disrespectful because they show people behaving inappropriately or illegally – or are racist, bigoted or unkind. Show your respect for others by avoiding these sites. If you visit one by accident, close it and tell your teacher or an adult.
- Show respect for others' privacy by not trying to get into their online spaces without invitation, by not stalking them or copying their pictures.

3. Looking after property:

- By not stealing other people's property. It's easy to download music, games and movies, but piracy (downloading media that you have not bought) is just the name given to stealing online.
- By not sharing the music, movies, games and other software that you own with other people.
- By checking that the information you are using is correct. Anyone can say anything on the web, so you need to check that the research is correct by using reliable sites. When in doubt ask your teacher or your parents.
- By looking after other people's websites, acting appropriately when visiting them, not making changes or vandalising them, and reporting any damage that you find.
- By signing this agreement, I undertake to always act in a manner that is respectful to myself and others, to act appropriately in a moral and ethical manner.

4. Basic principles

- I will use the facilities for the purpose they were intended, my posts, comments and content will have an educational focus.
- I will respect and protect myself and others by ensuring that the content I add to my website shows me, my peers, the school and the wider community in the best light and perspective.
- I will not endanger myself or my peers by posting material that could put me or them at risk.
- I will moderate all comments posted on my blog. I will remove comments that are inappropriate or could cause offence to other people
- I will ensure that the material I upload does not violate anyone's intellectual property and I will acknowledge the source of my materials.
- I will, in all matters, conduct myself as a young adult acting in a moral and ethical manner.
- I will always report abuse or inappropriate behaviour to safeguard my safety and the safety of my peers and community.
- I understand that all material published is not private and is subject to view by a wide range of people, including members of the school as well as the wider community.

Borrowed Device Care

What is the best way to clean the screen? Use a soft, dry, lint-free cloth when cleaning the computer. If necessary, the cloth may be dampened slightly to assist in cleaning areas that do not appear to be coming clean with dry cloth.

Keep liquids away from your device. As tempting as it might be to drink coffee, soda, water or any other liquid near your laptop, accidents can happen all too easily. Alternatively, use a cup with a cover on it, so even if it does spill, the liquid doesn't go anywhere. Spilled liquids may damage the internal microelectronic components or cause electrical damage. Short circuits can corrupt data or even permanently destroy some parts of the laptop. The solution is very simple: Keep your drinks away from your computer. Even if you are careful, someone else might spill your drink.

Keep food away from your device. Don't eat over your laptop, the crumbs can fall between the keys and provide an invitation to small bugs or damage the circuitry. Worse yet, the laptop will look dirty if there are crumbs on it.

Do not use your device in a room where there are animals. Their fur and hair can get into the internal workings and damage them. Also larger animals (e.g dogs) can accidentally damage them by knocking them off their support.

Ideally keep the device in a clean and dust free room.

Always have clean hands when using your device. Clean hands make it easier to use your device and there will be less risk of leaving dirt and other stains on the computer. In addition, if you clean your hands before you use the device, you will reduce wear and tear on the coating caused by contact with sweat and small particles that can act upon the device's exterior.

Protect the display monitor. When you closing your device, make sure there are no small items, such as a pencil or small ear-phones, on the keyboard. These can damage the display screen if it is shut on them; the screen will scratch if the item is rough. Close the lid gently by holding it in the middle. Closing the lid using only one side causes pressure on that hinge, and over time can cause it to bend and snap.

Hold and lift the device by its base/edge, not by its LCD display (the screen). If you lift it by the screen alone, you could damage the display or the hinges attaching the display to the base or apply heavy pressure. The display is also easily scratched or damaged by direct pressure – take care not to place pressure on it.

Don't pull on the power cord. Tugging your power cord from the power socket rather than pulling directly on the plug can cause the cord to break off from the plug or damage the power socket. Also, if the power cord is near your feet, avoid kicking it accidentally; in fact, it is best to refrain from bumping into the plug at all because you could loosen it and eventually break it.

Be careful not to roll your chair over the charging cord. Stick the cord onto your desk with tape.

Be sure to plug accessory devices into their proper slots. Always look at the symbols on the laptop carefully before inserting devices. Jamming a USB drive in upside down may damage the socket, requiring replacement.

Don't expose your device to rapid temperature changes. When bringing your device indoors during winter, don't turn it on immediately. Instead, let it warm to room temperature first. This will avoid any potential for damage to the disk drive from condensation forming inside the machine. Avoid heat from sunlight as well. Don't leave your device in a car. Not only do the insides of cars experience large temperature swings that could damage electronics, but a laptop or tablet is an inviting target for a smash and grab thief.

Avoid placing heavy materials, such as books, on top of your device. This can push the LCD screen into the keyboard, and will eventually damage it.

Use a properly-sized carrying case. Make sure the carrying case you use is large enough to hold the device. This will help avoid scratching, squeezing or potentially dropping it. Many breaks happen because devices are dropped or bumped. A carrying case greatly reduces the risk of damage.

Only use and store your device in a well-ventilated area. When you are using your device, do so in a place that has a constant air-circulation. Lots of people ruin their devices by using them in enclosed areas and thus cause it to overheat.

Try to keep the device on a flat, clean surface. This prevents damage to the device. This can be hard to do, particularly if you are outside with your device, but if there is a flat surface available then put your device on it.

Don't use your device on the bed. Repeated use of a device on the bed will cause the fans to suck up the dust and debris in the bed, ultimately blocking the fan.

St. Cecilia Catholic School

Borrowed Device Acceptable Use Policy Agreement

Borrowed Device Care & Acceptable Use Policy

We acknowledge receipt of the Borrowed Device Care and Acceptable Use Policy, understand it, and agree to adhere to the principles and procedures detailed within. We understand and accept the conditions stated in the Acceptable Use Policy and agree to hold blameless, and release from any liability, St. Cecilia Catholic School, the sponsoring school, its subcontractors, and employees. We understand that the Borrowed Device Acceptable Use Policy may be revised by the school to respond to the changing environment of web based computer technology; We agree to any revised conditions of the BDAUP. We understand that a network user is expected to use good judgment and follow the umbrella Technology Acceptable Use Policy printed in the student handbook published by the school. We further understand that any student who violates any provision of the Borrowed Device Acceptable Use Policy may lose all network privileges on the St. Cecilia Catholic School network and may be disciplined, as appropriate, for violations of the Student Code of Conduct. We understand that displaying work on the Internet makes the work available for viewing by any person around the world who has Internet access. We agree to follow the principles of digital citizenship outlined in this agreement and accept that failing to follow these tenets will have consequences within the school environment.

Please complete permissions for student participation in activities involving the St. Cecilia Catholic School 1:1 Borrowed Device Program:

We agree to accept and care for our assigned device:	Yes	No
My student may utilize the device and Internet access at school:	Yes	No
My student may collaborate with other students on the Internet:	Yes	No
My student may participate in distance learning activities:	Yes	No
We acknowledge that charges may be incurred for breakage.	Yes	No

NOTE: If any boxes are left unchecked or if this form is not returned to the school, it will be assumed that permission is granted. You must specifically check and sign this form to deny any access.

Parent signature: _____ **Date:** _____

Student signature: _____ **Date:** _____