



LOGANVILLE CHRISTIAN ACADEMY

TECHNOLOGY HANDBOOK
2023–2024

Loganville Christian Academy exists to prepare students
academically, spiritually, and socially for God's call on their lives.

OVERVIEW	3
USE OF TECHNOLOGY	3
TECHNOLOGY POLICY	3
TECHNOLOGY FEES	3
STUDENT RESPONSIBILITIES	4
DEVICES	5
DAILY EXPECTATIONS	5
LOST/STOLEN EQUIPMENT	5
DEVICE DAMAGE AND REPAIRS	5
CHECKOUT GUIDELINES	5
COLLECTION	6
STUDENT ACCESSIBILITY	6
VIOLATIONS AND DISCIPLINE	8
CLASSROOM INTERVENTIONS	8
PROGRESSIVE DISCIPLINE	8
PARENT/GUARDIAN RESPONSIBILITIES	9
SUPPORT INTERNET SAFETY ETIQUETTE	9
EMPLOYEE RESPONSIBILITIES	9
TECHNOLOGY AND COMMUNICATION	10
TERMS AND CONDITIONS	10
INTERNET SAFETY	10
TERMS AND CONDITIONS	10

OVERVIEW

Loganville Christian Academy recognizes that access to technology in the school, home, and community environment provides students with greater and more frequent opportunities to learn, engage, communicate, and develop the necessary skills to be career and college-ready in the 21st century.

USE OF TECHNOLOGY

A structured digital environment that is safe yet demanding will support students and teachers as they explore uses of technology, thereby enhancing student's engagement with content and promoting the development of self-directed, responsible lifelong learners and biblically-aligned digital citizens.

All students will have access to various technologies throughout their educational careers: these technologies span across various platforms including, but not limited to, Apple, Microsoft, Adobe, and Google. All students will be required to participate in the standard device program, which provides each student a device for educational use.

The following handbook provides students and their parents/guardians with information about the general use of technology, "ownership," rights, and responsibilities for possession, care, and expectations as a digital citizen.

Each school year, all students, their respective parents/guardians, and employees must agree to all policies listed in this handbook to utilize LCA technology resources, LCA network, and all other school-owned, technology-related items.

With this privilege and the extraordinary opportunity to explore digital resources comes responsibilities for each student and his/her parents/guardians. LCA will ensure that all students use technology and its access as an essential part of their learning experiences. Along with the efforts of parents/guardians, LCA will follow its policies in maintaining an environment that promotes ethical and responsible conduct in all electronic resource activities and uses.

TECHNOLOGY POLICY

TECHNOLOGY FEES

Each student is required to pay an annual, nonrefundable technology fee, classified by his or her grade level. The fee schedule is listed below:

- PreK3 – 1st Grade: \$250
- 2nd – 12th Grade: \$350

This fee helps provide access to wireless and wired networking throughout campus, use and access Student Information System software (FACTS SIS), email, specialized curriculum software (STEM, Robotics, Bio-Med, etc.), student file storage, IT Help Desk support and training, and system-wide efforts that include upgrades, repairs, maintenance, and ongoing costs to support the use of technology at Loganville Christian Academy.

For Lower School, this includes sustainability and support of Chromebooks, iPads, technology in the Lower School STEM Lab, and other various experiences on campus.

For Upper School, this includes Learning Management Software (iLearn) and a school-owned, student-issued device.

For device repair costs related to damage and loss, LCA will charge for the entire repair or replacement cost of the device if damage or loss occurs due to the intentional acts or as the result of their negligence in handling the device.

For school-owned devices and peripherals, an asset tag is a barcode-like sticker placed on the device for inventory and monitoring purposes. Tags may not be modified or tampered with in any way. A student may be charged up to the full replacement cost of a device for tampering with a school asset tag or turning in a device without a school asset tag, as this may render the device unidentifiable and may not be able to be identified back to the original assigned user.

STUDENT RESPONSIBILITIES

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities that students accept when they use a school-owned (herein referenced as “Device”). In general, use of technology requires efficient, ethical, and legal utilization of all digital resources. Violations of these rules and guidelines will result in disciplinary action. The student will assume responsibility for:

1. Carrying Devices in a Safe and Secure Manner

The student is responsible for ensuring the following precautions:

- Transporting the Device in safe/secure bag/backpack/sleeve.
- Ensuring proper care is given when setting down bookbag (as this can damage the screen or body of the Device).
- Transporting Device with care and with the screen closed.
- Never lifting Device by the screen.
- Always placing Device in a sleeve/bag when moving from classroom to classroom or any other location.

2. Device Security

- When not in the student’s possession, Device(s) and its accessories are required to be placed in a secure location.
- Under no circumstances should Devices or accessories be left unattended in unsupervised areas.
- Unsupervised areas include the bathrooms, cafeteria, computer labs, hallways, Library/Media Center, unlocked classrooms, unlocked locker rooms, or any other area deemed insecure. Any Device left in these areas is in danger of being stolen or tampered with by unauthorized individuals. If a device is found in an unsupervised area, it should be taken immediately to the IT Help Desk.
- Devices are not allowed in the lunchroom when food or drink is being served, or this is done so at the risk of the student.

3. General Care

The student is responsible for ensuring the following precautions:

- Never leaving a Device unattended.
- Never loaning the Device or its accessories to another student.
- Keeping the Device on a flat, solid surface.
- Never setting books or stacking heavy objects on top of the Device.
- Never setting food or drink next to Device.
- Never leaving the Device exposed to direct sunlight, extreme temperatures, or moisture sources for extended periods of time.
- Always carefully insert cords and removable storage devices into the Device.
- Never defacing the device and its accessories by writing, drawing, coloring, stickers, etc.
- Never removing any logo, branding, serial numbers, stickers, or other ID tags on the device.

4. Screen Care

A Device screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure, heat, and light. The student is responsible for ensuring the following screen precautions:

- Never putting pressure on the top of a Device when it is closed.
- Never storing a Device with the screen open.
- Always making sure there is nothing on the keyboard before closing the lid (e.g., pens, pencils, etc.)
- Only clean the Device screen with a soft, dry microfiber cloth or antistatic cloth.

5. Problems/Repair

In the event a student-assigned Device is not functioning properly, is physically damaged, or otherwise, the student is required to take the device to the IT Help Desk located on the main floor of the Upper School building upon realization. If the device cannot be fixed immediately, the student will be issued a loaner device on a temporary basis. This device may or may not have the same functions as their assigned device; no exceptions can be made to this rule. A student will be responsible for any damage to or loss of the Loaned Device; all policies listed in this handbook apply to the student during the loaner period.

The student is responsible for ensuring the following:

- The student will never attempt to repair or reconfigure any Device.
- The student will not attempt to open or tamper with the internal components of the Device nor should the student remove any screws; doing so will render the manufacturer's warranty void.
- The student and parent/guardian will NEVER take a school-owned Device to an outside computer service for any type of repairs or maintenance; doing so may render the manufacturer's warranty void.

6. Appropriate Classroom, Library, and Study Hall/Instructional Focus Routines

When at school, the student will use the device and/or any of the school's technology equipment primarily for educational purposes. Using the device for recreational use during instructional time is not permitted unless explicitly allowed by teachers. Students are expected to participate fully in all classroom activities as directed by their teachers. In addition to the rules and guidelines set in this handbook, students must abide by all rules and guidelines set by the classroom teachers.

Violation of any responsibilities in this section will result in disciplinary action.

DAILY EXPECTATIONS

It is expected that all students and parents fulfill their responsibilities as defined in this handbook.

There is an expectation that:

- Students must bring their Device to school every day that classes are in session, charged and ready to be used.
- Students hold and maintain responsibility for ensuring their Device is charged prior to school each day.
- Students who leave their Device at home have an opportunity to checkout a device for that day and are responsible for returning it at the stated time when checking out device or else incur fines.
- Students may bring a personal wireless mouse and earbuds/headphones as needed. LCA assumes no responsibility in the provision or maintenance of these personal devices.
- Students will not deface their issued Device including the use of stickers, markers, paint, etc.
- Students will not damage their Devices intentionally.
- Students will only have their school issued Device on campus. No outside devices (with the exception of phones) are permitted.

LOST/STOLEN EQUIPMENT

If any Device, Device charger, or Device accessories (also, Equipment) is lost, the student and/or parent/guardian must report the loss to the school immediately. Reports should be filed with the IT Help Desk upon realization. The circumstances of each situation involving lost equipment will be investigated individually. Students may be billed for lost equipment.

If any Equipment is stolen, a police report must be filed and a copy of the report must be provided to the school by the student and/or parent/guardian in a timely manner. If there is not clear evidence of theft or the equipment has been stolen due to student negligence, the student and parent/guardian will be responsible for the full cost of replacement.

Loganville Christian Academy may use its discretion to replace a device if, and only if, it is determined by LCA that the student acted in a reasonable manner when storing and taking care of the device and acted in good faith to find the device, such as filing a police report and reporting the loss or theft to LCA. LCA will not be obligated to replace a device in the case of negligence and failure to use diligence with LCA property.

DEVICE DAMAGE AND REPAIRS

In the event that the device is inoperable via technical issue, damage, or otherwise, a temporary device may be checked out from the IT Help Desk.

CHECKOUT GUIDELINES

The following guidelines apply when a device or accessory is checkout from the IT Help Desk:

- The temporary loan of an LCA device/charger must be returned to the IT Help Desk no later than 3:30 p.m. that day.
- Loaners may not be checked out consecutively for longer than a three (3) day period of time unless other arrangements have been made in advance.
- Any device damaged by a student or while the Device is in his or her possession will be the financial responsibility of the student and applied to his or her account.

- Excessive checkouts (when a student’s device is not being repaired) may result in denial of the privilege.
- Students are permitted five (5) emergency checkouts per semester. After that, each checkout will result in a detention.

The following fines will be accrued when devices are not returned on time:

Device Type	Penalty Period Begins	Rate	Maximum Rate
Charger	24 hours after initial due date	\$5 / day	\$25
Chromebook/Windows Laptop	24 hours after initial due date	\$10 / day	\$350

Fines WILL NOT be removed when a device is returned. Borrowing a device is a privilege that is there to help in case of an emergency. Students who are not responsible and do not return devices or charges are taking away the opportunity for another student to use the school’s resources.

If the device, case, and/or power adapter has been damaged or defaced, the student will be fined respectively for the damage.

Failure to turn in the Device or pay any technology-related charges/fines will result in student record holds.

Replacement chargers, whether to replace a broken or lost charger or to purchase a spare, are available for purchase at \$25 each from the IT Help Desk and can be charged to the student’s respective account.

COLLECTION

The student’s Device, protective carrying case (if supplied), and Device charger must be returned if/when:

- The completion of the student’s final exams at the end of the school year.
- The student withdraws during the school year at any point.

Personal Devices

Phones/Smart/Bluetooth device policy is as follows:

- Middle School students (6th–8th grades) are required to turn in their phone or other personal device (i.e., an inactivated phone or media player) at the beginning of their first period class and will be picked up at either the conclusion of the day or upon being checked out for any reason. Middle School students who check in after first period must turn in their phone to the front office. High School students (9th–12th grades) are required, when in classes, to follow the policy of their instructors (i.e., device be placed in a bucket, in the student’s bag turned off, etc.). A fine will be imposed if the device policy is not followed. See the Family Handbook for the Valuable Personal Property policy/procedure.
- Smart watches are permitted, given they are not connected to any wireless connection (cellular, Wi-Fi, or otherwise), and may be requested to be taken off and put away for any reason.
- Personal devices (i.e., laptops outside of the LCA approved devices scope, phones, tablets, or any other device capable of connecting to a wireless connection) are not allowed to be connected to a student LCA network unless permitted by the IT Director and Principal.
- Students may not use external measures (i.e., a tablet with shared texting capabilities or other software that allows texting communication with SMS capabilities) to send Short Message Service messages (SMS), VoIP calls, or other messages including, but not limited to, iMessage, Google Hangouts, Slack, Jabber, Yammer, and QQ. Any student discovered using these services in class will be disciplined, outlined in the Violations and Discipline section.
- Earbuds/Airpod use is permitted only in class with teacher’s permissions. For the safety of all, use between classes is not permitted in hallways, outdoors, etc.

1. Logging into a Device

- The student will log into their Devices using their school-issued account.
- The student will never share account passwords with other students.

2. Managing and Saving Digital Work

- Most of the student work will be stored in Internet/cloud-based applications and can be accessed from any computer with an Internet connection and most mobile Internet devices.
- The student should always remember to save frequently when working on digital media. Not all applications have an auto-save function.
- The school is/will not be responsible for the loss of any student work.

3. **Listening to Music**
 - Any Device or personal device's sound must be muted at all times unless permission is obtained from a teacher.
 - Headphones may be used at the discretion of the teachers.
 - Students should have their own personal set of headphones for sanitary reasons.
4. **Watching Movies/TV Shows/Digital Media**
 - Watching movies, TV shows or any other digital media on devices is not allowed during school hours unless permission from the teacher has been provided to complete a school assignment.
5. **Webcams**
 - Webcams are to be used for educational purposes only, as determined under the direction of a teacher.
6. **Gaming**
 - Online gaming is not allowed during school hours unless the student has been given permission by a teacher.
7. **Backgrounds, Themes and Profile Pictures**
 - Inappropriate media may not be used as backgrounds, themes or school account profile pictures. The presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang-related symbols, or any other content deemed inappropriate by the administration will result in disciplinary actions.
 - The backgrounds on LCA-provided devices cannot be changed under any circumstances.
8. **Printing**
 - Students will be encouraged to publish and share their work digitally with their teachers and peers when appropriate.
 - Students are expected to print all homework at home. If a home printer is not available, printing will be available for school-related assignments. If this privilege is abused, a minimal per page fee may be incurred.
9. **Chrome Web Store**
 - Students are allowed to install approved Chrome Web Apps and Extensions from the Chrome Web Store.
 - Students are responsible for the Web Apps and Extensions they install on their Chromebooks. The downloading or manually installing (also, side loading) of inappropriate material will result in disciplinary action.
 - If a student desires to install a Web App or Extension that they do not have permissions to install, they can request for it to be approved themselves or ask a parent or teacher to have the app reviewed and approved to be installed.
 - Some Web Apps do not function the same way without an Internet connection. Please keep this in mind when traveling around without a connection.
10. **Removable Media**
 - Removable media can be defined as, but not limited to, CD, DVD, USB devices, camera flash media cards, and hard drives physically removed from their laptops or computer-based machines.
 - LCA has the right to pre-scan any removable media that an individual wants to bring into the LCA network to ensure that it is free of viruses and other unwanted malware and spyware. Extreme caution is to be exercised by any individual who uses removable media with regards to the safe handling and security of the removable device and its contents. No LCA confidential data is to be transported using removable media.
11. **Using Your Device and Account Outside of School**
 - Students are encouraged to use their Devices at home and other locations outside of school for educational purposes.
 - A Wi-Fi Internet connection will be required for the majority of use, as most applications exist on the Internet. However, some applications can be used while not connected to the Internet.
 - A Windows Device will be required to occasionally connect to the LCA network in order to reconnect with directory services. The Device may cease to allow logins if the device is removed from the LCA network for an extended period of time.
12. **Content Filter**
 - LCA utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All Devices, regardless of physical location, will have all Internet activity protected and monitored by LCA.

- Content filtering blocks the majority of unwanted content and continues to refine the algorithm it uses to improve protection daily.

13. Email Use

- An LCA email account is provided for all students through Google Workspace for Education. Email that originates from or is received by a school-owned computer or its contracted hosting company is the property of Loganville Christian Academy and can be used during a legal proceeding.
- Use of this account is a privilege and can be revoked at any time.
- Use of email accounts by students will align with the Student Handbook code of conduct, and the code will be used for discipline purposes.
- Students who use LCA-assigned accounts, including the school-provided Google Account, are expected to exhibit maturity and common sense.
- Students are responsible for messages sent from their accounts. Students should exercise extreme caution with their passwords and never let a fellow student use their accounts.
- Students will not identify their telephone numbers, home addresses, or any personal information in any email correspondence.
- Several student accounts are web-based and can be accessed outside the boundaries of our school; students are required to maintain the same behavior that is expected of them while in school.

The following restrictions have been set for email accounts on site:

<u>Grade</u>	<u>Incoming/Outgoing Messages</u>
PreK–2 nd Grade	Not Utilized
3 rd –10 th Grade	From/To Inside LCA Domain Only
11 th –12 th Grade	From/To Any Domain

- In the event a parent and/or guardian would like to email their student using their LCA-provided email account, the Student/Parent Email Communication Form can be filled out to allow cross communication. The form can be found on the IT parent portal (located in ParentsWeb).

Exceptions to any of these policies may be made as required to support educational efforts. Any effort to bypass or violate any responsibilities in this section will result in disciplinary action.

The use of any technology is a privilege and not a right. Students are expected to use technologies in accordance with this Technology Handbook, classroom rules, Electronic Network Access and Acceptable Use Policy, Student, and Parent/Guardian Technology Agreement, and any applicable local, state, and federal laws. Violations of these policies will result in disciplinary action and repossession of the device and its accessories. Administration may also refer the matter to law enforcement if the violation involves an illegal activity.

CLASSROOM INTERVENTIONS

For low-level violations, classroom interventions will be the first level of discipline. This includes, but is not limited to, verbal warnings, seating changes, loss of privilege to use the device during the class period, teacher contact with home, and any other intervention deemed appropriate for the violation(s). Documentation of these infractions along with intervention attempts will be recorded by the classroom teacher.

PROGRESSIVE DISCIPLINE

Discipline will be imposed on an escalating scale, ranging from a verbal warning to a possible expulsion, based on the number of previous violations and the nature of or circumstances surrounding a particular violation. If multiple offenses occur, a student may lose his or her privilege for a designated length of time or on a permanent basis. Progressive discipline will be handled by the administration after referral from classroom teachers.

PARENT/GUARDIAN RESPONSIBILITIES

LCA makes every effort to equip parents/guardians with the necessary tools and information to ensure the safe use of the Devices in the home and community. There are several responsibilities assumed by the parent/guardian, which are outlined below:

1. Sign the Student/Parent Technology Agreement

- In order for students to be issued a Device, a student and his or her respective parent/guardian must sign the Student/Parent Technology Agreement.

2. Attend a Student/Parent Device Orientation (*applies to rising 6th and 9th graders and new students*)

- In order for students to be issued a Device, a parent/guardian must attend a Student Device Training.

3. Accept Liability

- The parent/guardian and student are responsible for the cost of repair or replacement at the date of loss if the property is any of the following:
 - Not returned.
 - Intentionally damaged.
 - Lost because of negligence.
 - Stolen but not reported to school and police in a timely manner.

4. Monitor Student Use

- The parent/guardian must agree to monitor student use at home and in any setting that is not the school. The best way to keep a student safe and on-task is through parent/guardian presence and continuous involvement, which can be done by completion of the following actions:
 - Investigate and apply parental controls available through the home's Internet service provider and wireless router.
 - Develop a set of rules/expectations for device use at home and in the community. Some websites provide parent/child agreements for you to sign.
 - Only allow device use in common rooms of the home (e.g., living room or kitchen) and not in bedrooms.
 - Demonstrate a genuine interest in what the student is doing on the device.
 - Ask questions and request that they show you their work often.

SUPPORT INTERNET SAFETY ETIQUETTE

Internet safety is about helping your child use the Internet productively and practice safe, responsible online behavior. The following are a few basic guidelines to share with your child:

- Follow your family's rules about when and where to use the Internet.
- Be polite, kind, and respectful in all Internet communications and whenever accessing technology.
- Understand a website's rules and terms and know how to flag other users for misbehavior.
- Recognize "red flags," including someone asking personal questions such as your name and address. Encourage your child never to share his or her name, the school's name, his or her age, his or her phone number, or his or her email or home address with strangers.
- Never send pictures to strangers.
- Keep passwords private (except from parents).
- Never open a message from any unknown source; it may contain a virus that can harm a computer.
- Immediately tell an adult if something makes you feel uncomfortable or something suspicious happens.
- Visit Common Sense Education Connecting Families, a website designed to support and empower families in raising kids who think critically, participate responsibly, and behave ethically in their online lives.

In addition to all standards and responsibilities in this handbook for parents and students, employees are expected to:

- Utilize network and cloud storage for all files.
- Not store anything on the local drive or desktop.
- Never share ID/password for anything. This includes but is not limited to FACTS, iLearn, Windows, Google, Papercut, and Door Security.
- Always lock devices when leaving them unattended.

Employees are responsible for any device issued to them. This includes laptops, Chromebooks, iPads, etc. The employee will be held financially responsible for any damage, theft or loss to a device that has been issued to them.

User personal safety includes, but is not limited to:

1. Users will not post school-related personal information about themselves or others outside of the secure areas of the LCA network (i.e., on the public "Internet"). Personal information includes but is not limited to the following: name, address, profiles, telephone, date of birth, identifying pictures, or any other personally identifying information.

2. Users will not utilize LCA's technology assets to arrange for meetings with anyone they have met online without the knowledge of the school and permission of a parent/guardian.
3. Users will promptly disclose to their teacher or administrator any message they receive that is inappropriate or makes them feel uncomfortable.
4. Users will not harass another person or engage in personal attacks, including those prejudicial or discriminatory in nature, following the guidelines of LCA's anti-bullying policy.

INTERNET SAFETY

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this Authorization and otherwise follow this Authorization.

Staff members shall supervise students while students are using School Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this Authorization. LCA shall endeavor to provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

LCA's Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by LCA. (Note: The filtering device is not guaranteed to block all inappropriate sites. Even the most sophisticated and current technology tools cannot block all inappropriate sites 100 percent.)

TERMS AND CONDITIONS

1. Acceptable Use

Access to LCA's electronic networks must be for the purpose of education, research, or communication and be consistent with the educational objectives of LCA. LCA's systems and devices are provided to accomplish the primary goals of LCA. While some immediate and necessary personal access will take place with rare exception, all personal business is expected to take place on personal time, using personal equipment, and through the use of personally provided network access. Personal use is unacceptable and should be avoided on the LCA network and systems.

2. Privileges

The use of LCA's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or school administrators will make all decisions regarding whether or not a user has this authorization and may deny, revoke, or suspend access at any time.

3. Technology Etiquette

Technology etiquette shall be observed and utilized by all Users. Technology etiquette includes, but is not limited to, the following:

- Be polite! Do not get abusive in your messages to others.
- Exercise caution when using sarcasm and humor. Without face-to-face communications, a joke or statement may be misunderstood.
- Show consideration and respect for others at all times.
- Be respectful of the rights of other network users and do not violate their privacy.
- Be aware of the intent and function of an individual or group before sending a message.
- Deliberately posing as a user other than yourself is prohibited.
- At the conclusion of a user's session, the user should log off the system he or she is using.

Inappropriate language shall not be used in any LCA device communication. Inappropriate language includes, but is not limited to:

- Obscene, profane, lewd, vulgar, offensive, inflammatory, threatening, or disrespectful language.
- Participation in hate mail, harassment, discriminatory remarks, and other harmful or inappropriate behaviors.

Users will maintain a respect for privacy while using LCA system(s). Respect for privacy includes, but is not limited to:

- Not forwarding or posting a message that was sent to them privately without the consent of the person who sent it.
- Not posting private information about another person.
- Not interfering with other users' work or files.

4. Unacceptable Use

The user (i.e., student) is responsible for his or her actions and activities involving the network.

5. Inappropriate Access to Material

LCA Users will not seek inappropriate access to material while using LCA System(s). Inappropriate material is information that is:

- Profane or obscene (pornography).
- Advocates illegal or violent activities.
- Advocates discrimination towards other individuals or groups.

If a user inadvertently accesses inappropriate material, he or she should immediately notify his or her teacher or administrator, thereby avoiding an allegation of intentional violation of the Technology and Communication Device Acceptable Use Policy. Users will not deliberately attempt to override or circumvent the firewall or content filter or encourage others to do so.

6. Unacceptable Use

Unacceptable use of LCA Systems by any user can be defined as, but is not limited to, the following:

- Using the network for any illegal activity, including violation of copyright, violation of contractual rights, or transmitting any material in violation of any U.S. or state law.
- Using the network for commercial or private advertising.
- Using the network for private financial or commercial gain.
- Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused.
- Wastefully using resources, such as file space.
- Hacking or gaining unauthorized access to files, resources, or entities.
- Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature.
- Using the Internet and LCA resources in any way that would disrupt its use by others.
- Using another user's account or password.
- Intentional posting of material authored or created by another.
- Intentionally posting anonymous messages and/or misrepresenting one's own identity to others.
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
- Capturing, recording, or transmitting the words and or images of any student, staff member, or other person in the school without express prior notice and explicit consent.
- Using the network while access privileges are suspended or revoked, deleting data, hiding, or attempting to interfere with the discovery of a violation of this policy.
- Furthering personal causes such as political, religious, or commercial views.
- Disseminating threatening or harassing messages.
- Disseminating sexually explicit or otherwise inappropriate material.
- Attempting to gain unauthorized access to computers, servers, shared service accounts, voicemails, or other devices.
- Purposely infecting the network or devices with spyware, malware, or viruses.
- Gaining access by using another's credentials.
- Using the Internet to access bandwidth-grabbing programs unless authorized to do so.
- Violating copyright laws (anything from the Internet should be regarded as copyright protected and permission should be obtained for appropriate usage).
- Downloading or uploading any data or material not specifically related to your job function.
- Downloading, storing, creating, or forwarding any information/data that is inflammatory or defamatory to any race, creed, ethnicity, or religion of any individual or group.
- Downloading any unauthorized software, file, or program.
- Downloading, storing, creating, or forwarding any information regarding explosives or weapons unless as information for a specific and approved class assignment.
- Downloading, storing, creating, or forwarding any information regarding alcohol, tobacco, regulated drugs, or illegal drugs unless as information for a specific and approved class assignment.
- Playing unapproved games that have been downloaded onto a technology device or that are played on the Internet. Assigned, teacher-approved interactive tools, which are directly related to the curriculum, are permitted.
- Using the Internet or other technology media to access chat rooms (including those in games, instant messaging, or any online chat functions).
- Accessing personal accounts including, but not limited to, email, music, banking, shopping, and other personal accounts except where such use is severely limited to immediate and necessary access.
- Users' activities, projects, or materials developed with technology and devices of Loganville Christian Academy must reflect our educational standards and policies. This includes but is not limited to webpage designs,

PowerPoint presentations, radio broadcasts, or any other public or private representation of LCA.
Impersonating other individuals, real or fictional, unless this is part of an approved educational assignment done as part of the conduct of a class.

- Attempting to install or utilize any application to work around or bypass security and/or school policies (e.g., VPN, terminal services, and proxy).

7. Limitation of Liability

LCA makes no expressed or implied guarantees that the activities or services provided by LCA technology or devices will be error-free or without defect. LCA will not be responsible for any damages to users including, but not limited to, loss of data, interruptions of service, personal or psychological damages, or financial losses.

LCA is not responsible for the accuracy or quality of content obtained through our network or stored on our systems. Finally, LCA will not be responsible for unauthorized financial obligations incurred from use of our devices or any components of our technology system. LCA does maintain a general liability policy for the school.

LCA specifically denies any responsibility for the accuracy or quality of information obtained through its services.

8. Indemnification

The user agrees to indemnify LCA of any losses, costs, or damages, including reasonable attorney fees, incurred by LCA relating to, or arising out of, any breach of this Authorization, school policy, or rules and procedures.

9. Unauthorized Access

Users shall not tamper with or attempt to gain access to computer data for which the user has no security authorization. This includes, but is not limited to, financial, employee, or student information and documents.

10. Security

Network security is a high priority. The following will help to reduce the risk to our network:

- If you can identify a security problem on the Internet, you must notify the IT Office or a school administrator. Do not demonstrate the problem to other users. Any user identified as a security risk may be denied access to the network.
- Users should take all reasonable precautions to prevent others from gaining access to their account(s). All users are responsible for their individual account(s).
- If an individual suspects a possible security breach, the user will immediately contact his or her teacher, administrative supervisor, or IT director.
- Users will not disseminate passwords, access codes, telephone numbers, account numbers, grades, or other individuals' documents to unauthorized persons. Keep your account and password confidential. Do not use another individual's account. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges.
- Loganville Christian Academy's network, storage systems, including Google Drive, and related technologies are the property of LCA and are subject to inspection by LCA administrative officials at any time. Users should not have a privacy expectation in the contents of their personal files on the LCA network or on web-based systems that LCA has contracted with to provide storage or services. There is no guarantee or right to privacy of any electronic communication originated from or stored on the LCA network or system.
- LCA reserves the right to monitor or spot-check any Internet or device activities occurring on school equipment or accounts. Students agree to submit their devices, including devices owned by them or their parents that may be in their possession at LCA or on an LCA-sponsored activity, for inspection by an LCA administrator at any time. Any student not agreeing to submit his or her device for inspection shall have his or her device placed into electronic quarantine until it can be retrieved by a parent. Failure to agree to inspection and to be subject to this accountability may result in suspension or termination of the student.

11. Vandalism

Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network component. This includes, but is not limited to, the uploading or creation of computer viruses.

12. Copyright and Copyright Web Publishing Rules

Copyright law and LCA policy prohibit the republishing of text or graphics found on the web or on school websites or file servers without explicit written permission.

- Student work may only be published if there is written permission from both the parent/guardian and student.
- For each republication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission

was granted. If possible, the notice should also include the web address of the original source.

13. Use of Electronic Mail

LCA's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by LCA. LCA provides email to aid staff members in fulfilling their duties and responsibilities and to students as an education tool.

- LCA reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. The account user has no expectation of privacy with regard to any electronic mail account or other aspect of LCA's electronic mail system. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- Electronic messages transmitted via LCA's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the school. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of LCA.
- Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to computer services. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- Use of LCA's electronic mail system constitutes consent to these regulations.