Legacy Preparatory Charter Academy
Acceptable Use Policy and Technology Agreement

TECHNOLOGY RESOURCES

To prepare students for an increasingly technological society, Legacy Preparatory Charter Academy provides an array of technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence throughout the organization by facilitating resource sharing, innovation, creativity, and communication with the support and supervision of parents, teachers, and staff. The use of these technology resources is a privilege, not a right.

This agreement sets forth the standards governing LPCA's staff and student use of those technology resources. This agreement also sets forth the rules under which authorized users may continue their access to and use of the resources. This agreement promotes the ethical, legal, and school-related use of LPCA's Network and ensures Legacy Preparatory Charter Academy's compliance with the Children's Internet Protection Act. Personal electronic devices will be governed under this agreement when such devices are attached to the Network.

Access to computers brings the potential availability of material that may not be considered to be of educational value into school setting. LPCA firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the organization.

ORGANIZATIONAL RESPONSIBILITIES

Legacy Preparatory Charter Academy's Superintendent, Administrators, Technology Manager, and Teachers will serve to oversee the organization's system and will work with the Texas Education Agency, Region 10 Education Service Center, and other agencies as necessary to ensure the safety of all users of the Network and Internet.The Technology Department will establish a process for setting up individual accounts for storage of information, establish procedures for the storage of images, video, and music files, establish a training and information as needed, establish an organization wide virus protection process, and coordinate other activities related to the use of the Network.
The organization utilizes software designed to block access to certain Internet sites, and to monitor and log all activity of users on the Network, or otherwise act to verify or enforce compliance with the organization's policies and purposes.

Disclaimer:

Pursuant to the Children's Internet Protection Act, Legacy Preparatory Charter Academy uses filtering software to screen Internet sites for offensive material. The goal is to filter pages containing offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Obscene/indecent/Vulgar; and Illegal/Questionable. Innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address may lead to receipt of unsolicited e-mail containing offensive content. With this in mind, LPCA reminds authorized users that accessing the Internet is done at the risk of the user. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful, and children and staff gain access to inappropriate and/or harmful material, Legacy Preparatory Charter Academy will not be liable. To minimize these risks, staff and student use of the Network is governed by this agreement. Furthermore, staff and students are responsible for seeking assistance in the event they need help in safely conducting Internet searches.

Definition of Organization Technology Resources:

The Organization's computer systems and networks include any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), optical media, digital images, digitized information, communications technologies, and new technologies as they become available. The organization reserves the right to monitor/review all technology resource activity.

GENERAL PROVISIONS

Authorized Users:

All authorized users shall adhere to the provisions of this agreement (and any other applicable organizational policy, regulation, or administrative directive) as a condition for continued use of the Network. It is a general policy of Legacy Preparatory Charter Academy to promote the use of computers in a manner that is responsible, legal, and appropriate. This agreement is enacted anytime there is a connection to the Organization's hardwired or wireless network or from an outside line such as Fiber, T-1, BRI, PRI, VPN, Dialup, DSL, Distance Learning Equipment, and other personal electronic devices.

TERMS AND CONDITIONS FOR USE OF LPCA'S NETWORK AND HOTSPOTS AS AN EXTENSION OF LPCA'S NETWORK

Acceptable Uses:
LPCA staff and students may use the various resources provided by the Network to pursue educationally related activities consistent with the Organization's mission and goals. Commercial use of the Organization's system is strictly prohibited.
The organization will make training available to all users in the proper use of the system and a copy of the acceptable use guidelines is available in the LPCA Employee Handbook, the Student Code of Conduct and on the LPCA website. All training in the use of the Organization's system will emphasize the ethical use of this resource. Teachers and other staff should help guide students in their use of the Network so that students will learn how Internet resources such as discussion boards, wikis, and blogs can provide valuable educational information from classrooms, campuses, and other national and international sources. In addition to using the Network strictly for educational pursuits, authorized users will be expected to follow generally accepted rules of digital citizenship and network etiquette (also known as netiquette). These

include, but are not limited to, the following:

1. Use appropriate language.
2. Do not pretend to be someone else when sending or receiving messages.
3. Do not submit, publish, or display any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.
4. Never reveal personal information such as addresses or phone numbers of users or others without their knowledge or consent, or if not required to do so by law or duty.
5. Never use the network in such a way that would disrupt the use of the network by other users.
6. Be polite.
7. Follow existing copyright laws, copies of which may be found in each campus library.
8. Post only allowable Podcasts, Blogs, Forums, WIKIs and Streaming Media. Allowable items:
    a. Support of Organization goals and/or supports LPCA approved curriculum.
    b. Are student or teacher-created.
    c. Are loaded on an Organization's website or Organization approved resource.
9. Use only Applications (Apps) that:
    a. Support of Organization goals and/or the LPCA approved curriculum.
    b. Are not disruptive to Organization systems or applications.
    c. Do not incur unauthorized charges.
10. Electronic Mail provides a powerful and nearly instantaneous way to communicate and collaborate with people around the world.
    a. Students may be granted e-mail access only through an Organization approved e-mail system.
    b. Organization employees will be provided with an individual e-mail account.

While most people consider e-mail to be private, users of E-mail should clearly understand that the level of privacy afforded is actually much lower than for postal correspondence. Legacy Preparatory Charter Academy reserves the right to review all e-mail as it deems appropriate, including for purposes of enforcing adherence to the guidelines for use set forth in this Agreement, other Organization policies, or other legal requirements.

- The Organization is providing e-mail access for the purpose of furthering its educational mission. It is expected that members of the school community will make use of that access for educational purposes. Commercial use of the Organization's email access or other electronic communications access is not permitted.
- Organizationally issued E-Mail accounts are the property of Legacy Preparatory Charter Academy, upon ending employment, or withdrawing as a student, the E-Mail account will be deactivated, and all contents of the account will remain the property of LPCA.

Unacceptable Uses

Unacceptable uses of the Network include, but are not limited to:

1. Downloading or installing unauthorized games, programs, files, electronic media, and/or stand- alone applications from the Internet or placing external data on any computer, whether stand-alone or networked to the Organization's system, without permission from the Technology Department.
2. Attempting to log on or logging on to a computer or e-mail system by using another's password. Assisting others in violating this rule by sharing information or passwords is also unacceptable.
3. Attempting to bypass the Organization's communications system through the use of software, hardware, or outside proxy systems. Assisting others in violating this rule by sharing information or passwords is also unacceptable.
4. Bypassing the Internet filter by connecting an Organization device to an external network, including 3G/4G, while on LPCA property.
5. Improper use of any computer or the network. This includes the following:
    a. Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages, either public or private, to teachers, students, parents, or other individuals or groups.
    b. Using the network for cyber-bullying
    c. Using the network for financial gain, political, or commercial activity.
    d. Attempting to harm or harming equipment, materials, or data.
    e. Attempting to send or sending anonymous messages of any kind.
    f. Using the network to access inappropriate material.
    g. Knowingly placing a computer virus on a computer or the network.
    h. Using the network to provide addresses or other personal information that others may use inappropriately.
    i. Accessing information resources, files, and documents to which you have not been granted access or without authorization from another user.
6. Using inappropriate or impolite language.
7. Disclosing personal information, including the names, addresses, and telephone numbers of students or colleagues. If an LPCA employee receives a Public Information Act Request or Freedom of Information Act Request, the request must be immediately forwarded to the Superintendent.
8. Intentionally disrupting the use of the Network for other users, including, but not limited to, disruptive use of any processes or programs, utilizing tools for ascertaining passwords, participating in or commissioning a Distributable Denial of Service (DDoS) attack, or engaging in "hacking" of any kind.
9. Intentionally spreading computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a computer system without authorization or for damaging or altering the software components of a computer or computer system.
10. Disclosing the contents or existence of LPCA computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients.
11. Attempting to harm or destroy LPCA equipment or materials, data of another user of the Organization's system, or any of the agencies or other networks to which the Organization has access.

System Access

Access to the Organization's network systems will be governed as follows:

1. Student and staff members are the only authorized user of their assigned device.
2. Students and staff members will have access to the Organization's resources for class assignments and research.
3. Students and staff members will be responsible for the integrity of their accounts by keeping passwords confidential and will not allow another user access to their account.
4. Any system user identified as a security risk or having violated the Acceptable use Agreement may be denied access to the Organization's system. Other consequences including discipline or adverse employment action, as applicable may also occur. See "Sanctions" below.
5. Any system user having been denied access rights may be reinstated with a limited access account to reduce the level of security risk to the system. Limits on this type of account may include time limitations, station access limitations, file access restrictions, and a revocation of Internet access privileges.
6. Personal devices may only be connected to the Organization network via wired or wireless connection with express permission from the technology department and may not be used as a replacement or in lieu of Organization provided devices.
7. Student and staff members may be allowed network access using their personal devices. This access may be revoked at any time by the Technology Department.

Campus Level Responsibilities

The campus director or designee will:

1. Be responsible for disseminating, collecting signed permission forms, and enforcing the Acceptable Use Agreement.
2. Ensure that employees supervising students who use the Organization's systems provide information emphasizing the appropriate and ethical use of this resource.

Individual User Responsibilities

The following standards will apply to all users of the Organization's computer network systems:

1. The user in whose name a system account is issued will be responsible at all times for its proper use. If a user feels that a password has been compromised, the user is responsible for immediately making a report to an administrator.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by Organization guidelines.
3. Users may not use another person's system account.
4. Any App purchased with a LPCA account will become the property of LPCA.
5. Users, if granted access to electronic mail, are asked to archive or delete electronic mail consistent with the Organization's retention policies.
6. Users are asked to delete unneeded files from the Organization servers on a regular basis.
7. Users will be responsible for the care and condition of their computer systems. If a computer system assigned to the user becomes damaged, the user can be held fiscally responsible for replacement or repairing the computer system. (See Sanctions Below)
8. Maintenance issues should be reported to the Technology Department immediately using the established procedures.
9. Campus issued devices should never be taken to an outside service repair provider. All repairs must be done through the authorization of the Technology Department.

Users will be responsible for following all copyright laws.

All authorized users are to promptly report any breaches of security, violations of acceptable use, (including inadvertent access to prohibited sites), and the transmission of web addresses or e-mail information containing inappropriate material to the campus director or LPCA Technology staff member. Failure to report any incident promptly may subject the authorized user to corrective action consistent with the Disciplinary Code, Organization policies, or applicable directives.

Intentional attempts to degrade or disrupt system performance may be viewed as violations of LPCA guidelines and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes but is not limited to uploading or creating of computer viruses, system break-in utilities, DDoS attacks, or system hacking programs. Vandalism as defined above will result in the cancellation of system use privileges and possible criminal prosecution. The party will be responsible for restitution of costs associated with system restoration, hardware, or software costs.

Authorized User Websites

The Organization will establish a Web site and will develop Web pages that will present information about the Organization. The Organization will have a designated Webmaster, responsible for maintaining the Organization Web site.

Campuses and classes are encouraged to establish Web pages that present information about the campus or class activities. LPCA's technology department will be responsible for managing the organization's web site. All sites must be for educational purposes.

Only authorized users may create web pages as a part of a campus or class activity. Material presented on an authorized users' website must meet the educational objectives of the class activity. LPCA reserves the absolute right to exercise control over the content and/or style of the authorized users' web pages.
Only those students whose parent(s) or guardian(s) have completed the Consent and Release Form may post their work or picture on student or campus websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only for confidentiality and safety purposes.

Monitoring

The Network is routinely monitored to maintain efficiency. Authorized users should be aware that use of the Network, including e-mail, is subject to monitoring by the LPCA Technology Department and designated administrators. Any activities related to or in support of violations of this agreement (or other Organization policy) may

be reported and will subject the user to sanctions specified either in the Student Code of Conduct, this agreement, other applicable Organization policy, or administrative directives.

Assumption of Risk

LPCA will make a good faith effort to keep the Network system and its available information accurate. However, authorized users acknowledge the following:

- There is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available.
- LPCA is not liable for lost or corrupted data. While LPCA utilizes backup software, users are encouraged to safeguard important files.
- LPCA does not warrant that the Network will be error free or free of computer viruses.
- LPCA is not responsible for any damage, physical or software based, that is incurred to personal devices while connected to the Network.
- In making use of these resources, authorized users agree to release LPCA from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the Network.
- The information available through the Internet may be inaccurate. LPCA has no ability to maintain such information and has no authority over these materials. LPCA makes no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of the data and/or information residing on or passing through the Network from outside networks.
- Use of the Network is at the risk of the authorized user.

Social Media Policy

Social media is a communication tool in the form of websites or applications that staff and students use to share information and exchange ideas. LPCA understands the value of social media and encourages its use with the understanding that guidelines will be in place to protect the organization's approved accounts/pages.
Users are responsible for their own behavior when communicating with social media. They will be held accountable for the content of the communications that they state/post on social media.

Users are responsible for complying with the Organizational employee, student and conduct policies. Users may not disrupt the learning atmosphere, educational programs, campus activities, and the rights of others.
The Organization has the right, but not the duty, to inspect, review, retain, or remove electronic communication
created, sent, displayed, received or stored on and over the Organization's network and to monitor, record, check, track, log, access or otherwise inspect its network system.

The Organization is not held accountable for any content published using a personal social media account.

Social Media Guidelines – Student

This Administrative Regulation applies to all Campus environments, whether the social media is used on Campus property, or beyond Campus property (including but not limited to, at a third-party's contracted property).
In addition to the regulations provided in the Organization's Social Media Policy, some guidelines include but are not limited to the following. The Organization reserves the right to determine if any guideline not appearing in the list below constitutes acceptable or unacceptable social media use.

- Students must not promote or appear to promote illegal drugs, illegal activities, violence, drinking, and cyber bullying.
- Students must not impersonate or access another user's account/page with or without permission.
- Students should state/post only what they want the world to see. Imagine your parents, teachers, and administrators visiting your social media. Essentially, once a student shares something it is likely available after (s)he removes it from the social media and could remain on the internet permanently.
- Students should comply with the rules that have been established for the Organization's educational social media when they use it.

Indemnification

The authorized user indemnifies and holds LPCA harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the Network that cause direct or indirect damage to the user, LPCA, or third parties.

Sanctions

Students

Failure to abide by this agreement may subject the authorized Student user to corrective action ranging from suspension of some or all access privileges up to and including expulsion and prosecutions according to the Student Code of Conduct.

- If access to the Network is revoked by a campus faculty member the Student user has the right to appeal the revocation within thirty (30) days, in writing, to the director of the campus.
- If access to the Network is suspended by the LPCA Technology Department, the Student user may appeal the suspension to the Campus Director or designee.
- Once an authorized user is removed from the Network, there shall be no obligation to provide a subsequent opportunity to access the Network.
- Student can be held financially liable for damaging district resources. If the student does damage a computer device, there is no obligation for LPCA to reinstate access to any district technology resources.

PARENT
I have read the Organization's Acceptable use Technology Agreement and its associated administrative regulations. In consideration for the privilege of my child using the

Organization's technology resources, I hereby release the Organization, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, these resources, including, without limitation, the type of damage identified in the Organization's policy and administrative regulations.

- I give permission for my child to access the Organization's technology resources and certify that the information contained on this form is correct.

Parent Signature: AcceptableUseParentSign Date: AcceptableUseParentDate
Student Signature: AcceptableUseStudentSign Date: AcceptableUseStudentDate