

# Little Cypress Mauriceville C.I.S.D.

## Student Code of Responsible Computing and Use of Technology

Little Cypress Mauriceville CISD provides access to the Internet and the District's electronic communications systems for students, teachers, and staff for educational purposes. Access will be used to enhance learning consistent with the District's educational goals.

The District's computer systems and networks (system) are any configuration of hardware and software. The electronic communications system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers and network equipment;
- Computer hardware (including mobile devices, tablets, i-devices) and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, video and audio files;
- Internally or externally accessed databases, applications, or tools (Online/Internet – or District-server based);
- District-provided filtered Internet access;
- District-provided filtered guest and WiFi; and
- New technologies as they become available.

These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have serious consequences, harming the District, its students and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District system users and setting standards which will serve to protect the District.

In order for the District to be able to continue to make its Network and Internet access available, all users must take responsibility for appropriate and lawful use of this access. Users must understand that one person's misuse of the District technology hardware or software, Network and/or Internet access may jeopardize the ability of all to enjoy this access. While the District's management and network administrators will make reasonable efforts to administer use of the Network and Internet access, they must have user cooperation in exercising and promoting responsible use of this access.

Access to the District's electronic communications systems is a privilege, not a right. Administrators and faculty may review files and messages to maintain system integrity, to ensure that users are acting responsibly. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing the use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. To educate students on proper computer/network/Internet use and conduct, students are required to review these guidelines at the beginning of each school year. Employees supervising students who use the District's system must provide training emphasizing its appropriate use.

Access to the District's electronic communication system, including the Internet, shall be made available to staff and students for instructional purposes. Each District computer and guest Wi-Fi (available for staff and students who bring their own approved personal telecommunication devices) has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA. However, while the District uses filtering technology and protection measures to restrict access to inappropriate material; it is not possible

# Little Cypress Mauriceville C.I.S.D.

## Student Code of Responsible Computing and Use of Technology

to absolutely prevent such access. It is each student's responsibility to follow the rules of appropriate and responsible use.

Student Access is provided to all students unless parents or guardians request in writing to the campus principal that access be denied. Student internet access will be under the direction and guidance of a district staff member. Students may also be allowed to use the local network and guest Wi-Fi with campus permission.

For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for educational software tools. Parents wishing to deny access to these educational tools must do so in writing to the campus principal indicating their child should be denied access to these tools. Examples of these tools are Discovery Education, District cloud-computing services, Prezi, blogs, and Edmodo.

Students may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and online meeting sessions. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. These tools should not be considered a private, personal form of communication. All users should assure that they do not share personally identifiable information online. Verbal or written language considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools.

Electronic communication is an important skill for 21<sup>st</sup> Century Students. By providing this tool, the District is equipping students with the skills necessary for success in the business world or academic endeavors. Students in grades 3-12 may be given access to a District student email account. Parents wishing to deny access to District email must do so in writing to the campus principal. As appropriate, project email accounts may be granted for educational activities for students in grades K-5 at the request of the classroom teacher. Student email accounts may be provided directly by the District, through the content management system of an approved online course, or through a district-approved provider.

A student or staff member who gains access to any inappropriate or harmful material is expected to discontinue access and to report the incident to the supervising staff member. Any user identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

Staff, students, and parents of students with access to the District's systems should be aware that use of the systems may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

Appropriate Use:

- If you are assigned an individual account for hardware and Internet access, you are responsible for not sharing the password with others.
- You are responsible for any activity that occurs under the use of your account login. If you leave your device or user account unattended and logged in with the device unlocked, and inappropriate activity occurs, you may be held responsible for that activity.
- You may not give your login information to another user (Exception: you may provide it to the technical support personnel for support purposes, but you are responsible for changing it after they assist you and resolve your issue.)

# Little Cypress Mauriceville C.I.S.D.

## Student Code of Responsible Computing and Use of Technology

- You will be held responsible at all times for the proper use of District technology resources, and the District may suspend or revoke your access if you violate the rules.
- Your account is to be used primarily for educational purposes.

### Inappropriate Use:

- Includes, but is not limited to, those uses that violate the law, that are specifically named as violations in policy, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it.
- Transmission of any material in violation of any federal or state law is prohibited. This includes but is not limited to:
  - Threatening, harassing, defamatory or obscene material;
  - Copyrighted material;
  - Plagiarized material;
  - Blog posts, web posts, or discussion forum/replies posted to the Internet which violate federal or state law.
- Modifying or changing computer settings and/or Internal or external configurations without appropriate permission is prohibited.

Any malicious attempt to harm or destroy District equipment, materials or data, or the malicious attempt to harm or destroy data of another user on the District's system, or any of the agencies or other networks to which the District has access, is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Users may not redistribute, forward or share confidential information without proper authorization.

- Students must respect others' right to privacy.
- Students must not transmit, redistribute, or forward to outside individuals not expressly authorized to receive the information.
- Students must not send messages, post documents, or participate in educational activities using a false identity, or use the accounts of others.
- Students will not access files, folders, or other electronic data of others without permission.
- Students will not add, modify, or delete electronic system resources or configurations without permission.
- Students will not use the Internet for financial gain, commercial activity, or political activity.
- Students will not use LCMCISD electronic resources to purchase products or services.
- Students will not redistribute copyrighted programs or data without the written permission of the copyright holder.
- Students will not engage in Cyberbullying. Cyberbullying includes but is not limited to, harassing, disrespecting, impersonating, tricking, and cyber stalking.
- Students will not reveal personal information about themselves or others such as, home addresses, phone numbers, email addresses, or birthdates.
- Students should not respond to requests for personally identifying information or contact from unknown individuals.
- Students should not meet in person with people met online. If a request for such a meeting is received, it should be reported to a teacher or administrator immediately.

# Little Cypress Mauriceville C.I.S.D.

## Student Code of Responsible Computing and Use of Technology

- Students will use appropriate language for the educational environment and for the educational activity in which they are currently involved. (Examples of inappropriate language include: swearing, ethnic or racial slurs, or any other inflammatory or threatening language.)
- Students will be held responsible at all times for the proper use of District technology resources, and the District may suspend or revoke your access if you violate the rules.
- Students will not access the control panel on a district computer, or attempt to modify settings in any way.
- Students will not access Proxy server websites that are designed for, intended to, or by chance scan our network, or attempt in any way to circumvent our security.
- Students will not open, send, or receive obscene pictures or messages.
- Students will not upload any personal media files to any shared network folder, device, and/or the network that are not for educational purposes.
- Students will not use LCMCISD Technology resources for any non-instructional or inappropriate purpose. (Examples include: online gaming, Facebook, blogs, wikis, etc.)
- Students will not knowingly infect a computer or network with a virus.
- Students will not install any software, viruses, or games on any district computer or system connected to district networks without permission from the teacher.
- Students will not attempt to harm equipment, materials, or data.
- Students will not log into a computer for another student whose access has been suspended.
- Students will always report any known violations of the LCMCISD Acceptable Use Guidelines to their teacher or an administrator. If they have identified a possible security problem, the Technology department should be notified immediately.
- Students will not waste district resources through improper use of the system. (Examples include: printing personal material, modifying computer settings.)

### Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

District users are bound by all portions of the Responsible Use Guidelines. A student who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved Student Code of Conduct. With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

### Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

# Little Cypress Mauriceville C.I.S.D.

## Student Code of Responsible Computing and Use of Technology

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

### BYOT (Bring Your Own Technology)

The District believes technology is a powerful tool that enhances learning and enables students to access a vast amount of academic resources. The District's goal is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. As resources are available, the District will open a filtered, wireless network through which students in specific age groups will be able to connect privately owned (personal) telecommunication devices. Students using personal telecommunication devices must follow the guidelines stated in this document while on school property, attending any school-sponsored activity, or using the LCMCISD network.

Students are allowed to bring their own devices provided they have received written permission from the Principal **and** Technology Director. Attendance at a BYOT training session provided by the District is required. Personal devices must also have current virus protection and all system updates done on a regular basis. The District is not responsible for the personal devices owned by the student, or the applications and information stored on the devices. The District cannot be held responsible for any possible device charges to your account that might be incurred during approved school-related use. The form for students to request the use of personal technology can be found at: <http://www.lcmcisd.org/tech/docs/PersonalDevicesStudent.pdf> Electronic devices will not be used as a factor in grading or assessing student work.

General usage guidelines follow:

**High School**– Students are allowed to bring personal telecommunication devices that can access the Internet for educational purposes as determined by the classroom teacher. Use of personal devices must be approved by the Principal and Technology Director. Students will be allowed to use the device between classes and in the cafeteria setting in a digitally responsible manner.

**Junior High** – Students are allowed to bring personal telecommunication devices that can access the Internet for educational purposes as determined by the classroom teacher. Use of personal devices must be approved by the Principal and Technology Director. Students will not be allowed to use the devices during passing periods or in the cafeteria setting.

**Elementary** – Students in grades 3-5 are allowed to bring personal telecommunication devices for academic classroom use as determined by the classroom teacher. Use of personal devices must be approved by the Principal and Technology Director.

# Little Cypress Mauriceville C.I.S.D.

## Student Code of Responsible Computing and Use of Technology

### User Acknowledgement Required

Each user authorized to access the District computers, networks, telecommunications, Internet services, or other resources is required to sign a Responsible Use Guidelines Acknowledgement form.

**Students:** Please print the student's legal name (first, middle, and last) in the space provided below:

First Name: \_\_\_\_\_

Middle Name: \_\_\_\_\_

Last Name: \_\_\_\_\_

Please have the student sign in the space provided below:

Student's Signature: \_\_\_\_\_

Please print student's grade level: (K-12) in the space provided: \_\_\_\_\_

**Parents:** I understand the importance of the technology rules and will support the Student Code of Responsible Computing and Use of Technology. Elementary students will only access Internet sites selected by their teachers and will view selected sites with the teacher present. Parents or guardians of students guilty of damaging property will be liable for damages in accordance with the law.

Each user authorized to access the District computers, networks, telecommunications, Internet services, or other resources is required to sign a Responsible Use Guidelines Acknowledgement form, or the Employee or Student Code of Conduct and Student/Parent Handbook Acknowledgement Form stating that they have read policy CQ Local, CA Legal and CQ Exhibit (the Responsible Use Guidelines)

I understand that Computer/Network/Internet access is provided to all students unless parents or guardians request in writing to the campus principal that access be denied.

Parent's Signature: \_\_\_\_\_ Date: \_\_\_\_\_