LYCÉE FRANÇAIS

DE LA NOUVELLE-ORLÉANS

CHILDREN'S INTERNET PROTECTION ACT (CIPA) - COMPLIANCE POLICY

COMPUTER AND TECHNOLOGY POLICY

Lycée Français (LFNO) network access is a privilege, not a right; any violation of the following will result in forfeiture of permission to use the Internet and school network and appropriate disciplinary action.

All hardware and software used in the school is the property of the school, not the student. As such, students have no reasonable expectation of privacy to any information saved on or transmitted through any part of the school's network.

Respect for the school's equipment and network is a condition for use of a computer. Students may not deliberately damage the network or any part of the network's systems. Restitution is required for any damage incurred.

TERMS AND CONDITIONS FOR COMPUTER AND INTERNET USE

1. *Acceptable Use* – Limits are placed by Lycée Français on the use of LFNO computers, LFNO network and the Internet under the terms of Acceptable Use. Only those uses that are acceptable as defined in this policy are allowed when accessing these resources.

2. *Netiquette* - Users shall be expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not send abusive messages to others. Use appropriate language.

b. Do not reveal personal addresses or phone numbers of students or colleagues.

c. Note that Electronic Mail (EMail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities must be reported to the authorities. All users should be aware that routine monitoring of the system may lead to discovery that the user has or is violating the Acceptable Use Agreement, the Student Handbook and/or the law. Routine maintenance of the system may also purge files from individual accounts.

d. Do not use the network in a way that would disrupt the use of the network by other users (e.g. downloading large files - generally over 1 gigabyte (1GB) during school hours, sending mass email messages, or excessive or otherwise unwanted contact of other users via chat or other instant messaging apps on the network). Hardware or software shall not be destroyed, modified, or abused in any way.

e. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system shall be prohibited.

f. Hate mail, harassment, discriminatory remarks and other antisocial behaviors shall be prohibited on the network.

g. The illegal installation of copyrighted software for use on district computers shall be prohibited.

h. Use of the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the local area network (LAN) shall be prohibited.

3. *Privileges* - The use of the Internet is a privilege, not a right, and inappropriate use shall result in a cancellation of those privileges and may result in disciplinary or legal action by the administration, faculty, or staff.

4. *Security* - Security on any computer system is a high priority, especially when the system involves many users. Any suspected security problem on the Internet shall be reported to the Director of Technology or designee, who shall inform the Principal of serious incidents. Any user identified as a security risk or having a history of problems with other computer systems shall be denied access to the Internet.

5. *Vandalism* - Vandalism is defined as any malicious attempt to harm or destroy hardware or software data of the school system, another user, the Internet Service Provider, or other networks that are connected to Internet. This includes, but is not limited to, the uploading or creation of computer viruses, defacing Websites, unauthorized changes to websites, programs, applications, databases, etc. Vandalism shall result in cancellation of privileges and / or other disciplinary actions up to and including expulsion.

6. *Unauthorized Software* – Defined as software that has not been approved by the Director of Technology. No software, programs, or system files (fonts, drivers, etc) may be installed or downloaded by any user without the prior permission of the Director of Technology, who must scan for appropriateness and viruses.

7. *Consequences of Misuse* - School principals and district administrators may discipline (up to and including expulsion) any student who breaches or violates this Acceptable Use policy.

8. *Cyber Bullying* – In the State of Louisiana, Cyber bullying is defined in state law and is punishable under the law. The law defines Cyberbullying as:

"the transmission of any electronic textual, visual, written, or oral communication with the malicious and willful intent to coerce, abuse, torment, or intimidate a person under the age of eighteen."
Ref: LA Rev Stat § 14:40.7

INTERNET SAFETY

Intent - In accordance with the Children's Internet Protection Act (CIPA), the Lycée Français Board ("School Board") shall enforce a policy of Internet safety. It is the intent of Lycée Français (LFNO) to advance and promote education, collaboration and exchange of information among students in a safe and nurturing environment. The LFNO network is provided for students to conduct research, complete assignments, and communicate with others. The purpose of Internet access in this context is to support education and research in and among academicians and students by providing access to valuable educational tools, unique resources and opportunities for collaborative work. Access to the Internet for educational purposes when appropriate, will enable students to use thousands of libraries, databases, scientific resources, museums and cultural resources. Within reason, freedom of speech and access to information will be honored.

While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. Lycée Français believes that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed the disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

Filtering – On the LFNO campus networks, Lycée Français implements technologies that incorporate blocking or filtering of certain Internet content through the use of network security equipment or security services. Examples of the type of content subject to these restrictions include certain visual depictions, including without limitation those that are obscene, child pornography, or otherwise harmful to minors. Sites that are excessively, violent, pervasively vulgar, sexually harassing, or that contain information regarding the manufacturing of bombs or other incendiary devices shall also be prohibited. Only authorized persons may disable the blocking or filtering mechanism for an adult user in order to enable Internet access for bona fide research or other lawful purposes. While filtering software is in use, no filtering system is capable of blocking 100% of the inappropriate material available on the Internet. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Monitoring and Training - In addition to the use of technology to implement protective measures, Lycée Français will implement processes deemed necessary and appropriate to monitor student's online activities and access to the Internet and World Wide Web. Such monitoring may include, but shall not be limited to, the following:

1. Ensuring the presence of a teacher and/or other appropriate school personnel when students are accessing the Internet including, but not limited to, the supervision of students when using electronic mail, chat rooms, instant messaging and other forms of direct electronic communications. As determined by the appropriate administrator, the use of e-mail and chat rooms, instant messaging and other forms of direct electronic communications may be blocked as deemed necessary to ensure the safety of such students.

2. Monitoring logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors.

3. Provide annual training regarding CIPA policy to all students and a minimum of 4 hours annually to all faculty staff. Training for students and faculty will address key issues such as cyber bullying, social networking dangers and emerging technologies that may endanger children while using the Internet. Teachers will train students by incorporating within their lesson plans age appropriate Internet Safety training for students. Teachers will access training materials from sites such as http://commonsense.org. The curriculum specialist or the designated representative will periodically review lesson plans to ensure all students are trained.

Ref: 47 USC Section 254 (Telecommunications Act), Pub. L. 106-554 (Children's Internet Protection Act), La. Rev. Stat. Ann. §17:81, 17:100.7, 17:280.

PROHIBITIONS

In addition to filtering and monitoring policies, it shall be the policy of the School Board to:

1. Prohibit access by minors on the Internet and World Wide Web to inappropriate matter as outlined in the section TERMS AND CONDITIONS FOR COMPUTER AND INTERNET USE above;

2. Institute measures to ensure the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications, such as "Instant Messaging";

3. Prohibit unauthorized access, including what is now known as hacking, and other unlawful on-line activities by minors online;

4. Prohibit transmission of any material in violation of any U.S., state, local or School District regulations,

5. Prohibit unauthorized disclosure, use, and dissemination of personal information regarding minors; and

6. Institute measures designed to restrict minors' access to materials harmful to minors.

PERMISSIONS

Parental/guardian permissions that are assumed include:

1. Access to the Internet.

2. Permission to publish students' work to classroom websites.

3. Permission to have unidentified photos of students published to classroom web sites as per the LFNO media release, except in cases where release was not granted.

ACCEPTABLE USE

It is the intent of Lycée Français to advance and promote education, collaboration and exchange of information. Successful operation of Internet and other related technological services requires that, as in life, all people regard our shared environment as a shared resource. It is, therefore, imperative that all users conduct themselves in a responsible, ethical, and polite manner.

LFNO Network Use

The LFNO network is provided for students to conduct research, complete assignments, and communicate with others. As access to network services is given to students, they are expected to act in a considerate and responsible manner. Students are responsible for good behavior on school computer laptops, tablets, Chromebooks and networks just as they are in a classroom or a school hallway. Access is a privilege - not a right. As such, general school rules for behavior and communications apply. Beyond the clarification of such standards, Lycée Français is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.

Network storage areas are similar to school desks. Network administrators may review files and communications to maintain system integrity and ensure that the system is used responsibly. Users should expect that files stored on LFNO servers will be accessible by the school's administrators.

Internet / World Wide Web Safety

- Students may not view, download or transmit any offensive, inappropriate or illegal material. Students must notify their teacher immediately of any disturbing material they may encounter online.
- Students may not illegally download or host (offer for upload) copyrighted material or software nor make unauthorized copies of any software, music or other material.
- Students may not gamble on the network or use the network for commercial purposes, lobbying or advertising.
- Students may never give out or publish personal information over the Internet.
- Students may not share passwords or allow other students to use their school accounts.
- Students may not visit or download files from File Sharing or Social Media (Facebook, SnapChat, Pinterest, Twitter, etc...)