La Porte Independent School District

Employee Application/Agreement for Network/Internet Account

Employee's Full Name: ______________________________ _________________

School/Facility: ___________________________________ Room/Office: ______________

Employee's Job Title: ____

I understand and will voluntarily abide by **La Porte Independent School District's Network/Internet Acceptable Use Guidelines.**

I further understand that any violation of the guideline is unethical and may constitute a criminal offense. Should I commit such violations, my access privileges may be revoked. In addition, school disciplinary action and/or appropriate legal action may be taken.

My signature indicates that I have read the **La Porte Independent School District's Network/Internet Acceptable Use Guidelines** carefully, understand its significance, and voluntarily agree to comply fully with all terms and conditions therein.

Employee Signature: _____________________________________ Date: _______________

Please complete and return to your campus/department secretary.

Computer/Network/Internet
Acceptable Use Guidelines

La Porte Independent School District makes a variety of communications and information technologies available District employees through computer**,** network, and Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication within the District. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District. These Acceptable Use Guidelines are intended to minimize the likelihood of such harm by educating District employees and setting standards which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the District's computer systems and networks far outweigh any disadvantages.

Mandatory Review. To educate District employees on proper system use and conduct, users are required to review these guidelines at the beginning of each school year. All District employees shall be required to acknowledge receipt and understanding of all administrative regulations and Acceptable Use Guidelines governing use of the system and shall agree in writing to comply with such regulations and guidelines and to allow monitoring of their use of the system.

Definition of District Technology System. The District's computer systems and networks (technology system or system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail facilities;
- Electronic mail (e-mail) accounts;
- Fax machines;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, e-mail, digital images and audio files;
- Internally accessed databases or tools;
- Externally accessed databases (such as the Internet); and,
- New technologies as they become available.

Availability of Access

Acceptable Use. Computer/Network/Internet access will be used to improve teaching consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/network/Internet use.

Privilege. Access to the District's system is a privilege, not a right.

Access to Computer/Network/Internet. System access is provided to all District teachers and staff.

Access to the District's electronic communications system, including the Internet, shall be made available to employees primarily for instructional and administrative purposes and in accordance with these Acceptable Use Guidelines. Limited personal use by District personnel is permitted if the use imposes no tangible cost to the District, does not unduly burden the District's computer or network resources, and has no adverse affect on an employee's job performance.

All individual users of the District's system must complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the Human Resources office/Campus.

System users are required to maintain password confidentiality by not sharing their password with others. System users may not use another person's system account.

Any system user identified as a security risk or having violated the District's Administrative Regulations and/or these Acceptable Use Guidelines governing use of the system may be denied access to the District's system. Other consequences may also be assigned.

Content/Third-Party Supplied Information. System users with access to the District's network should be aware that its use may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material.

An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Subject to Monitoring. District computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. System users should not use the computer system to send, receive or store any information, including e-mail messages, that they consider personal or confidential and wish to keep private. All electronic files, including e-mail messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose.

User Responsibilities

Computer/Network/Internet users are responsible for their actions in accessing available resources.

Employee Responsibilities. District employees are bound by all portions of the District's Acceptable Use Guidelines. An employee who knowingly violates any portion of the Acceptable Use Guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Campus- and Departmental-Level Responsibilities. The principal/departmental administrator or designee will:

1. Be responsible for disseminating and enforcing the District's Acceptable Use Guidelines for the District's system at the campus or departmental level.
2. Ensure that all individual users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in Human Resources or campus administrative offices.
3. Ensure that employees supervising students who use the District's systems provide information emphasizing its appropriate responsible and ethical use.
4. Assist in monitoring all users of the District's systems to ensure appropriate and ethical use.
5. Use the District's student management system to identify students who do not have permission to use the Internet and inform staff members who are responsible for these students that they do not have permission to use the Internet.

Teacher Responsibilities. The teacher will:

1. Provide lessons in Internet safety and cyber security for students.
2. Review responsibilities as users of the District computer/network/Internet prior to gaining access to such system.
3. Provide developmentally-appropriate guidance to students as they use electronic resources related to instructional goals.
4. Use computer/network/Internet in support of instructional goals.
5. Provide alternate activities for students who do not have permission to use the Internet.
6. Treat student violations of the District's Acceptable Use Guidelines as defined in the *Student Code of Conduct*.
7. Use streaming media (audio and video) for educationally-appropriate purposes.

La Porte ISD Employee Code of Conduct. District employees are expected to maintain appropriate conduct when accessing the communications and information technologies available through the District's technology system. All employees must comply with the District's Acceptable Use Guidelines at all times when accessing any part of the technology system.

Employees will guard and protect access to secure systems by:

1. Protecting passwords and other similar authorization information. Passwords are the primary way in which users are authenticated and allowed to use the District's computing resources. Employees will not disclose personal password(s) to any individual, including a faculty or staff member. Similarly, employees will not disclose other identifying information used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.
2. Guarding unauthorized use of resources. Employees will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied. Staff members should lock their computer when leaving their work station.
3. Not circumventing or compromising security. Employees must not utilize any hardware or software in an attempt to compromise the security of the District's system or use access to the District's system to compromise or circumvent the security of another system. Examples of prohibited activities include (but are not limited to) use or placement of Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and intentional transmission of viruses or worms.

System usage **(including computer, network, and Internet access)** is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the District for any purpose. Employees will affirm, in writing, that at all times their actions while using the District's system will not violate the law or the generally accepted rules of network etiquette, will conform to the guidelines set forth in the Acceptable Use Guidelines, and will not violate or hamper the integrity or security of the District's technology system.

If a violation of the Acceptable Use Guidelines occurs, employees will be subject to one or more of the following actions:

1. Revocation of access;
2. Disciplinary action;
3. Loss of employment with the District;
4. Appropriate legal action.

Use of Social Networking/Digital Tools. Online communication is an asset to employee learning of 21st century skills. Students and employees may participate in social media learning environments and use digital tools such as, but not limited to, blogs, discussion forums, RSS feeds, podcasts, wikis, and message boards with pre-approval from the District.

Use of System Resources. System users are asked to purge e-mail or outdated files on a regular basis to be in compliance with electronic records retention policies.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of the system or any components that are connected to it. The following actions are considered inappropriate uses and are prohibited:

Violations of Law. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- copyrighted material;
- plagiarized material;
- threatening, harassing, defamatory or obscene material; or
- material protected by trade secret.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws.

Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the investigation or litigation processes.

Intellectual Property. Teachers and staff must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, dissemination, or transfer of others' materials without appropriate authorization is not allowed.

Transmitting Confidential Information. Teachers and staff may not redistribute or forward confidential information (i.e. educational records, personally identifiable information from education records, directory information, personnel records, etc.) without proper authorization as defined in Board Policies FL(legal), FL(local), and DBA(legal). Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing such personal information as home addresses or phone numbers of users or others is prohibited.

Modification of Computer. Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Commercial Use. Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-LPISD Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief. Any attempt to harm or destroy District equipment, materials or data; or the attempt to harm or destroy data of another user of 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.

Vandalism/Criminal Mischief as defined above is prohibited and will result in the cancellation of system use privileges. System users committing vandalism/criminal mischief will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See DH, FN series, and FO series in Board Policy]

Impersonation/Plagiarism. Fraudulently altering or copying documents or files authored by another individual or assuming the identity of another individual is prohibited.

Illegally Accessing or Hacking Violations. Intentional unauthorized access or attempted unauthorized access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

Copyright Violations. Downloading or using copyrighted information without following approved District procedures is prohibited. Approved District procedures for downloading and/or using copyrighted information can be found on the LPISD web site.

System Interference/Alteration. Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Cyber Bullying. Cyber bullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures or images, or website postings (including blogs) which has the effect of:

- Physically, emotionally or mentally harming a student;
- Placing a student in reasonable fear of physical, emotional or mental harm;
- Placing a student in reasonable fear of damage to or loss of personal property; or

Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

Electronic Mail

Electronic mail (e-mail) is one of the most used communications tools in the District. It should be used primarily for instructional and administrative needs. All teachers and staff are issued e-mail accounts. Users should check e-mail frequently, delete unwanted messages promptly, and stay within the e-mail server space allocations. E-mail attachments may be limited to a specific size should system resource availability require it. Internet access to personal e-mail accounts is not allowed. E-mail is archived in accordance with Federal laws.

Employees should keep the following points in mind:

Perceived Representation. Using school-related e-mail addresses might cause some recipients or other readers of the e-mail to assume that the user's comments represent the District or school, whether or not that was the user's intention.

Privacy. E-mail communication should not be considered a private, personal form of communication. The District has the right to access, monitor, review, copy, modify, delete or disclose such files for any purpose**.** Private information, such as home addresses or phone numbers, should not be divulged in e-mail without the permission of the individual involved.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in e-mails distributed through District e-mail is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Political Lobbying. Consistent with State ethics laws, District resources and equipment, including, but not limited to, e-mail, must not be used to conduct any political activities, including political advertising or lobbying. This includes using District e-mail to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of e-mails, hyperlinks, or other external references within e-mails regarding any political advertising.

Forgery. Forgery or attempted forgery of e-mail messages is prohibited. Attempts to read, delete, copy or modify the e-mail of other system users, deliberate interference with the ability of other system users to send/receive e-mail, or the use of another person’s user ID and/or password is prohibited.

Junk Mail/Chain Letters. Users should refrain from forwarding e-mails which do not relate to the educational purposes of the District. Chain letters or other e-mails intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

Use of non-District devices

The use of non-District devices is expressly forbidden without prior approval from the Technology Department.

District Web Contributor Responsibilities

The purpose of District Web sites is to communicate campus, department, and District activities and information to District Web patrons and employees. All official school and District Web sites must be hosted on a District Web server. All individuals creating/editing content for display on District Web servers are considered District Web-content contributors.

The District's Technology and the District's Communications Departments are responsible for ensuring that all Web-site contents, including but not limited to lpisd.org, campus Webs and teacher Webs, conform to the guidelines described below, as well the District's overall communications objectives. As such, the Communications Department reserves the right to alter or delete any content contained on a District Web site in order to ensure that it conforms with both Web- site guidelines and the District's communications objectives.

Content Issues

For the requirements below, "content" is defined as text, graphics, media, or other information that is visible and/or audible on a District Web page.

- All content must be approved by principals/department heads or their designees
- If any content and/or file [that is saved on a District Web server or content on an external (non-District ISD) Web site to which a hyperlink from a District Web page refers] exhibits any of the following conditions or presents any of the following problems, the individual responsible for that content will be asked to eliminate the offending condition within a reasonable amount of time. If the condition is not corrected after a reasonable amount of time, the District's Technology Department will take action to rectify the situation. An employee who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Content shall not be displayed if it:

- Contains questionable and/or inappropriate material and/or themes as defined in these guidelines and Board Policies CQ(legal) and CQ(local).
- Is of a personal nature.
- Includes commercial, trademarked, and/or copyrighted material without the express written consent of the "owner" of the content. If consent is obtained, the proper trademark/copyright symbol and/or owner's credits must be displayed.
- Is out-of-date or inaccurate.
- Contains hyperlinks that do not return an active Web page and displays a "Page Not Found".

- Contains hyperlinks that do not return a document and displays a “Page Not Found”.

Teachers must only use Web sites on District Web servers to post class information; however, teachers are allowed to post information related to curriculum projects using District-approved blog and wiki sites. A hyperlink from a teacher Web site to a teacher’s external, personal Web site or of any other external (non-District) Web site maintained by District staff or volunteers is prohibited.

Personal information about District employees and/or parent volunteers will not be disclosed without the approval of the individual and the principal/administrator and will be in accordance with District/campus procedures. Non-District e-mail addresses, non-District mailing addresses, and non-District phone numbers will not be disclosed on District/campus Web sites.

Pictures and names of employees and/or parent volunteers are allowed with their written approval.

Display of Student Information on District Websites

The following conditions apply to the display of student information on District Web sites. A content contributor who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

- Student-created projects, writings, and/or artwork are permitted on campus/District Web sites, or District-approved blog and wiki sites, if the appropriate parental consent has been obtained.
- Student photographs and names are permitted if the Publications, Video, Internet Consent and Release Agreement granting such consent for the student has been signed and is on file.
- All student photographs and/or student work must be displayed with either no name, first name only, or first name and last initial only. No other personal student information is allowed including, but not limited to, e-mail address, phone number, home address, and/or birth date.

Hyperlinks

The following requirements must be met to utilize hyperlinks on any District Web page. If these conditions are not met, the individual responsible for those hyperlinks will be asked to eliminate the offending condition within a reasonable amount of time, after which the District’s Technology Department will take action to rectify the situation. If the condition is a violation of (or promotes the violation of) any District policy or regulation or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content and/or file may be recommended.

- Hyperlinks to external (non-District) Web sites must include the following text on the District Web page where the hyperlink exists: “La Porte ISD is not responsible for content on external sites or servers.”
- Hyperlinks to all external (non-District) Web sites must open those Web sites in a new window.
- Hyperlinks to external (non-District) Web sites are only allowed where the content in those Web sites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide (as defined in these Guidelines) service to District Web patrons. However, if the content in these Web sites is judged unsuitable at any time, the hyperlink to the site will be removed.

- Hyperlinks to Web sites, whose content is prohibited by the District's Web filtering system, will not be allowed.
- Hyperlinks to District employee or volunteer personal Web sites are not allowed.

Special Features

There are special website features that will not be allowed on District Web sites.

- "Guestbooks", "chat areas", "message boards", or similar non-District, unmonitored, and/or user-community developed/maintained facilities are prohibited unless the employee is using a District-approved blog or wiki site for curriculum projects.
- No executable programs or applets are allowed on District Web sites.

Security

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the user should immediately notify the District's Help Desk. The security problem should not be shared with others.

Impersonation. Attempts to log on to the system impersonating a system administrator or District employee, student, or individual other than oneself, will result in revocation of the user's access to computer/network/Internet, and discipline in accordance with this document and/or Board Policy.

Other Security Risks. Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the District computer/network/Internet or other technology systems.

Consequences of Agreement Violation

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

Denial, Revocation, or Suspension of Access Privileges. The System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that attempts to block 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. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting. The La Porte Internet connection is the only system to be used in schools. No commercial Internet accounts may be used.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express 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.

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.