Lake-Lehman School District
ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION (CIS) SYSTEMS

1. Purpose

The Lake-Lehman School District ("School District") provides employees, students, and Guests ("Users") with hardware, software, access to the School District's Electronic Communications System and network, which includes Internet access, whether wired, wireless, virtual, cloud, or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, Board members, vendors, and consultants.

Computers, network, Internet, Electronic Communications, information systems, databases, files, software, and media, (collectively "CIS systems"), provide vast, diverse and unique resources. The Board of School Directors will provide access to the School District's CIS systems for Users if there is a specific School District-related purpose to access information; to research; to collaborate; to facilitate learning and teaching; and/or to foster the Educational Purpose and mission of the School District.

For Users, the School District's CIS systems must be used for Educational Purposes and/or performance of School District job duties. Students may only use the CIS systems for Educational Purposes. CIS systems may include School District Computers which are located or installed on School District property, at School District events, connected to the School District's network, or when using its mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another Internet service provider ("ISP"), and, if relevant, when Users bring and use their own personal Computers or personal electronic devices, and, if relevant, when Users bring and use another entity's Computer or electronic device, to a School District location, event, or connect it to a School District network. If Users' bring personal Computers or personal technology devices onto the School District's property, or to School District events, or connect them to the School District's network and systems, and if the School District reasonably believes the personal Computers and personal electronic devices contain School District information or contain information that violates a School District policy, or the legal rights of the School District or another person, or involves significant harm to the School District or another person, or involves a criminal activity, then the personal Computers or personal electronic devices may be legally accessed to insure compliance with this policy, and other School District policies, regulations, rules, and procedures, and ISP, local, state, and federal laws. Users may not use their personal Computers and personal electronic devices to access the School District's intranet, Internet or any other CIS System unless approved by the Director of Technology and/or designee and/or authorized as part of the School District's services provided to Users.

The School District intends to strictly protect its CIS systems against harm or outside and internal risks and vulnerabilities. Users are important and critical players in protecting these School District assets and in lessening the risks that can destroy these important and critical assets. Consequently, Users are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Superintendent and/or designee. Noncompliance will result in actions, further described in the "Consequences for Inappropriate, Unauthorized and Illegal Use" section found in the last section of this policy, and as provided in other relevant School District policies, regulations, rules, and regulations.

2. Definitions

1. Child Pornography - Under federal law, means any Visual Depiction, including any photograph, film, video, picture, or Computer or Computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. The production of such Visual Depiction involves the use of a Minor engaging in sexually explicit conduct;

b. Such Visual Depiction is a digital image, Computer image, or Computer generated image that is, or is indistinguishable from, that of a Minor engaging in sexually explicit conduct; or

c. Such Visual Depiction has been created, adapted, or modified to appear that an identifiable Minor is engaging in sexually explicit conduct.

Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, Computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited Sexual Act or in the simulation of such act is guilty of a felony of the third degree.

2. Computer - includes any School District owned, leased or licensed or User-owned personal hardware, software, or other technology device used on School District premises or at School District events, or connected to the School District network, containing School District programs or School District or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. For example, Computer includes, but is not limited to, the School District's and a User's: desktop, notebook, netbook, powerbook, macbook, tablet PC, iPad, Kindle, eBook readers, laptop Computers, printers, facsimile machine, cables, modems and other peripherals, specialized electronic equipment used for students' special Educational Purposes, Global Positioning System (GPS) equipment, RFID, personal digital assistants (PDAs), iPods, MP3 players, thumb drives, cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities), telephones, mobile phones, or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, Pulse Pens, and any other such technology now existing or subsequently developed.

3. Electronic Communications Systems - any messaging, collaboration, publishing, broadcast, or distribution system that depends on Electronic Communications resources

to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across Electronic Communications network systems between or among individuals or groups, that is either explicitly denoted as a system for Electronic Communications or is implicitly used for such purposes. Further, an Electronic Communications system means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission/transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, wire or Electronic Communications, and any Computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, without limitation, the Internet, intranet, electronic mail services, voice mail services, tweeting, text messaging, instant messages, GPS, PDAs, facsimile machines, cell phones (with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities).

4. Educational Purpose - includes use of the CIS systems for classroom activities, professional or career development, and/or to support the School District's curriculum, policies, rules, and procedures, and mission statement.

5. Harmful to Minors - under Federal law, any picture, image, graphic image file or other Visual Depictions that:

a. Taken as a whole, with respect to Minors, appeals to the prurient interest in nudity, sex, or excretion;

b. Depicts, describes, or represents in a patently offensive way with respect to what is suitable for Minors, an actual or simulated Sexual Act or Sexual Content, actual or simulated normal or perverted Sexual Acts, or lewd exhibition of the genitals, and

c. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to Minors.

Under Pennsylvania law, that quality of any depiction or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

a. Predominantly appeals to the prurient, shameful, or morbid interest of Minors; and,

b. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for Minors; and,

c. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for Minors.

6. Inappropriate Matter - includes, but is not limited to visual, graphic, video, text and any other form of indecent, Obscene, pornographic, Child Pornographic, or other material that is Harmful to Minors, sexually explicit, or sexually suggestive. Examples include, taking, disseminating, transferring, or sharing Obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as sexting, e-mailing, texting, among others). Others include, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, flagging, terroristic material, and advocating the destruction of property.

7. Minor - for purposes of compliance with the federal Children's Internet Protection Act ("FedCIPA"), an individual who has not yet attained the age of seventeen (17). For other purposes, Minor shall mean the age of minority as defined in the relevant law.

8. Obscene - under federal law, analysis of the material meets the following elements:

a. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;

b. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be Obscene; and

c. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

Under Pennsylvania law, analysis of the material meets the following elements:

a. The average person, applying contemporary community standards, would find that the subject matter taken as a whole appeals to the prurient interest;

b. The subject matter depicts or describes in a patently offensive way, Sexual Conduct described in the law to be Obscene: and

c. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

9. Sexual Act, Sexual Contact and Sexual Conduct - are defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246(3), and 18 Pa.C.S.A. § 5903. 18 U.S.C. 2246; 18 Pa.C.S.A. § 5903(e)(3); 20 U.S.C. § 6777(e); 47 U.S.C. § 254(h)(7)(H).

10. Technology Protection Measure(s) - A specific technology that blocks or filters Internet access to Visual Depictions that are Obscene, Child Pornography or Harmful to Minors.

11. Visual Depictions - includes undeveloped film and videotape, and data stored on a Computer disk or by electronic means which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words.

3. Authority

1 . Access to the School District's CIS systems through school resources is a privilege, not a right. These CIS Systems and Resources, as well as the User accounts and information are the property of the School District. The School District, reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The School District will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems.

2. It is often necessary to access Users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and the right to access the stored communication of Users' accounts for any reason in order to uphold and enforce this policy and other School District policies, regulations, rules, procedures, the law, and to maintain the system. **USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE SCHOOL DISTRICT'S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE SCHOOL DISTRICT'S CIS SYSTEMS. The School District reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any or all CIS systems use and to monitor and allocate fileserver space.** Users of the School District's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the School District, and to the School Districts Monitoring and allocating fileserver space. Passwords and message delete functions do not restrict the school districts ability or right to access such communications or information.

3. The School District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the School District operates and enforces Technology Protection Measure(s) that block or filter online activities of Minors on its Computers used and accessible to adults and students so as to filter or block Inappropriate Matter as defined in this policy on the Internet. The Technology Protection Measure must be enforced during use of Computers with Internet access. Measures(s) designed to restrict adults' and Minors' access to material Harmful to Minors may be disabled to enable an adult or student (who has provided written consent from a parent or guardian) to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.

4. Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of written consent from a parent or guardian of a student, and upon the written request from an adult presented to the Director of Technology and/or Superintendent for Curriculum and Instruction.

5. The School District has the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, record, check, track, log, access or otherwise inspect; and/or to report all aspects of its CIS systems use. This includes any User's personal Computers, network, Internet, Electronic Communications systems, Computers, databases, files, software, and media that they bring onto School District property, or to School District events, that are connected to the School District network, or when using its mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and, if relevant, when Users bring and use their own personal Computers or personal electronic devices, and, if relevant, when Users bring and use another entity's Computer or electronic device to a School District location, event, or connect it to a School District network, and/or that contain School District programs, or School District or Users' data or information, all pursuant to the law, in order to ensure compliance with this policy, and other School District policies, regulations, rules and procedures, and ISP, local, state, and federal laws, to protect the School District's resources, and to comply with the law.

6. The School District reserves the right to restrict or limit usage of lower priority CIS systems and Computer uses when network and computing requirements exceed available capacity according to the following priorities:

a. Highest - uses that directly support the education of the students.

b. Medium - uses that indirectly benefit the education of the students.

c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications.

d. Forbidden - all activities in violation of this policy and/or local, state, and/or federal law.

7. The School District additionally reserves the right to:

a. Determine which CIS systems services will be provided through School District resources.

b. Determine the types of files that may be stored on School District file servers and Computers.

c. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and Electronic Communications Systems, including e-mail.

d. Remove excess e-mail or files taking up an inordinate amount of fileserver space after a reasonable time.

e. Revoke User privileges, remove User accounts, or refer violators to legal authorities and/or School district authorities when violation of this and any other applicable School District policies, regulations, rules, and procedures occur or ISP, local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, and destruction of School District resources and equipment.

4. Delegation of Responsibility

1. Due to the nature of the Internet as a global network connecting thousands of Computers around the world, Inappropriate Materials can be accessed through the network and Electronic Communications systems. Because of the nature of the technology that allows the Internet to operate, the School District cannot completely block access to these resources. Accessing these and similar types of resources will be considered an unacceptable use of School District resources and will result in actions explained further in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last Section of this policy, and as provided in relevant School District policies.

2. The School District must publish a current version of the Acceptable Use Policy so that all Users are informed of their responsibilities. A copy of this policy and *the CIS acknowledgement and Consent Form* must be provided to all Users, who must sign the School District's CIS Acknowledgement and Consent Form, by written means.

3. Users must be capable and able to use the School District's CIS systems, and software relevant to their responsibilities. In addition, Users must practice proper etiquette, School District ethics, and agree to the requirements of this policy.

4. The Director of Technology, and/or designee, will serve as the coordinator to oversee the School District's CIS systems and will work with other regional or state organizations as necessary, to educate Users, approve activities, provide leadership for proper training for all Users in the use of the CIS systems and the requirements of this policy, establish a system to insure adequate supervision of the CIS systems, maintain executed User *CIS Acknowledgement and Consent Forms,* and interpret and enforce this policy.

5. The Director of Technology and/or designees, will establish a process to set up individual and class accounts, set quotas for disk usage on the system, establish Records Retention and Records Destruction Policies and Records Retention Schedule to include electronically stored information (see School District Policy #800), and establish the School District virus protection process.

6. Unless otherwise denied for cause, student access to the CIS systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All Users have the responsibility to respect the rights of all other Users within the School District and School District CIS systems, and to abide by the policies, regulations, rules, and procedures established by the School District, its ISP, local, state and federal laws.

7. The Assistant Superintendent for Curriculum and Instruction, and/or designee(s), have the responsibility to educate Minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

5. Guidelines

1. Access to the CIS Systems

a. Users' CIS systems accounts must be used only by authorized owners of the accounts and only for authorized purposes.

b. An account will be made available to individual users according to a procedure to be developed by appropriate School District authorities.

c. CIS System. This Policy, as well as other relevant School District policies, regulations, rules, and procedures will govern use of the School District's CIS systems for Users.

d. Types of Services include, but are not limited to:

(1) Internet. School District employees, students, and Guests will have access to the internet through the School District's CIS systems, as needed.

(2) E-Mail. School District employees may be assigned individual e-mail accounts for work-related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Director of Technology and/or designees, and at the recommendation of the teacher who will also supervise the students' use of the e-mail service. Parents of students in the Lake-Lehman School District Virtual Academy must also supervise the child in his/her use of the School District's e-mail service.

(3) Guest Accounts. Guests may receive an individual web account with the approval of the Director of Technology and/or designees, if there is a specific School District-related purpose requiring such access. Use of the CIS systems by a Guest must be specifically limited to the School District-related purpose and must comply with this policy and all other School District policies, regulations, rules, and procedures, as well as ISP, terms, local, state and federal laws and must not damage the School District's CIS systems. A School District CIS Acknowledgement and Consent Forms must be signed in writing by a Guest, and if the Guest is a Minor a parent's written signature is required.

(4) Blogs. Employees may be permitted to have School District-sponsored blogs after having received training and the approval of the Director of Technology and/or designees. All Bloggers must follow the rules provided in this policy and other applicable policies, regulations, rules, and procedures of the School District.

(5) Web 2.0 Second Generation and Web 3.0 Third Generation Web-based Services. Certain School District authorized Second Generation and Third Generation Web-based services, such as, blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies, and interactive collaboration tools that emphasize online participatory learning (where Users share ideas, comment on one another's project, plan, design, or implement, advance or discuss practices, goals, and ideas together, co-create, collaborate and share) among Users may be permitted by the School District; however, such use must be approved by the Director of Technology and/or designees, followed by training authorized by the School District. Users must comply with this

policy as well as any other relevant policies, regulations, rules, and procedures, including copyright, participatory learning/collaborative/social networking during such use.

2. Parental Notification and Responsibility

The School District will notify the parents/guardians about the School District's CIS systems and the policies governing their use. This policy contains restrictions on accessing Inappropriate Matter. There is a wide range of material available on the internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the School District to monitor and enforce a wide range of social values in student use of the Internet. Further, the School District recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The School District will encourage parents to specify to their children what material is and is not acceptable for their children to access through the School's District's CIS system. Parents are responsible for monitoring their children's use of the School District's CIS systems when they are accessing the systems.

3. School District Limitation of Liability

The School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the School District's CIS systems will be error-free or without defect. The School District does not warrant the effectiveness of Internet filtering. The electronic information available to Users does not imply endorsement of the content by the School District. Nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The School District will not be responsible for any damage Users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the CIS systems. The School District will not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the School District's CIS systems. In no event will the School District be liable to the User for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems.

4. Prohibitions

The use of the School District's CIS systems for illegal, inappropriate, unacceptable, or unethical purposes by Users is prohibited. Any such activities engaged in by Users are strictly prohibited, including but not limited to these activities illustrated below. The School District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS systems.

These prohibitions are in effect any time School District resources are accessed, whether on School District property, through the Lake-Lehman School District Virtual Academy, at School District events, while connected to the School District's network, when using mobile commuting equipment, or telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and, if relevant, when an employee or student uses their own equipment.

Students are prohibited from visually possessing and using their personal electronic device or Computers, as defined in this policy, regulations, rules, and procedures, on School District premises and property (including but not limited to, buses and other vehicles), at School District events, or through connection to the School District CIS systems, unless expressed permission has been granted by a teacher or administrator, who will then assume the responsibility to supervise the student in its possession and use, or unless an IEP team determines otherwise, in which case, an employee will supervise the student in its possession and use. Thus, Users are prohibited from using cell phones, with or without Internet access, and/or recording or camera video devices and similar devices with similar and other capabilities and configurations. Cameras and the like may not be used to take images of others, transfer such images, or place such images on websites without the consent of the building administrator and the person whose photo is being taken. Students who are performing volunteer fire company, ambulance or rescue squad functions, or who need such a personal electronic device or Computer due to their medical condition or the medical condition of a member of their family, with notice and the approval of the school administrator, may qualify for an exemption to this prohibition.

a. General Prohibitions

Users are prohibited from using School District CIS systems to:

(1) Communicate about non-work or non-school related matters.

(2) Send, receive, view, download, store, access, print, post, distribute, or transmit material that is Harmful to Minors, indecent, Obscene, pornographic, Child Pornographic, terroristic, sexually explicit, or sexually suggestive. This includes, but is not limited to, Visual Depictions. Examples include, taking, disseminating, transferring, or sharing Obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as, sexting, e-mailing, texting, among others). Nor may Users advocate the destruction of property.

(3) Send, receive, view, download, store, access, print, distribute, or transmit Inappropriate Matter, as defined in this policy, or material likely to be offensive or objectionable to recipients.

(4) Cyberbully another individual or entity. See School District Bullying Policy #249.

(5) Gang up on a victim or target him/her or make him/her the subject of ridicule or aggression.

(6) Access or transmit gambling information or promote or participate in pools for money, including but not limited to basketball and football, or participate in any other betting activities or games of chance.

(7) Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate Matter in this policy.

(8) Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive, profane, or inflammatory communications.

(9) Participate in unauthorized Internet Relay Chats ("IRC's"), newsgroups, instant messaging communications and Internet voice

communications (on-line; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. Students must obtain consent from their teacher to use IRC's; however, even with such consent, they may not use instant messaging or text messaging. Employees may only use instant messaging if consent was obtained from the Director of technology, and/or designee.

(10) Use in an illegal manner or to facilitate any illegal activity.

(11) Communicate through e-mail for non-educational purposes or activities. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited (for example, the use of the everyone distribution list, building level distribution lists, or other e-mail distributions lists to offer personal items for sale is prohibited).

(12) Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable School District policies); conduct unauthorized fund raising or advertising on behalf of the School District or any non-school School District organization; engage in the resale of School District Computer resources to individuals or organizations; or use the School District's name in any unauthorized manner that would reflect negatively on the School District, its employees, or students. Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use. School District acquisition policies must be followed for School District purchase of goods or supplies through the School District system.

(13) Engage in political lobbying.

(14) Install, distribute, reproduce or use copyrighted software on School District Computers, or copy School District software to unauthorized Computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See the Copyright Infringement section in this Policy, the School District's Copyright Policy #8 14, and the School District's Copyright Guidelines Handbook for additional information.

(15) Plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.

(16) Install Computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on School District Computers is restricted to the Director of Technology and/or designees.

(17) Encrypt messages using encryption software that is not authorized by the school District from any access point on School District equipment or School District property. Users must use School District approved encryption to protect the confidentiality of sensitive or critical information in the School District's approved manner.

(18) Access, interfere, possess, or distribute confidential or private information without permission of the School District's administration.

Examples include accessing other students' accounts to obtain their grades or accessing other employees' accounts to obtain information.

(19) Violate the privacy or security of electronic information

(20) Send any School District information to another party, except in the ordinary course of business and as necessary or appropriate for the advancement of the School District's business or educational interest.

(21) Send unsolicited commercial electronic mail messages, also known as spam.

(22) Post personal or professional web pages without administrative approval.

(23) Post anonymous messages.

(24) Use the name of the "Lake-Lehman School District" in any form in blogs, on School District Internet pages or websites not owned or related to the School District, or in forums/discussion boards, and social networking websites to express or imply the position of the School District without the expressed, written permission of the Superintendent, and/or designee. When such permission is granted, the posting must state that the statement does not represent the position or endorsement of the School District.

(25) Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/proxies or any websites that mask the content the User is accessing or attempting to access.

(26) Advocate illegal drug use, whether expressly or through a latent pro-drug message. This does not include a restriction on political or social commentary on issues, such as the wisdom of the war on drugs or medicinal use of drugs.

(27) Attempt to and/or obtain personal information under false pretenses with the intent to defraud another person.

(28) Use location devices to ham or put another person in jeopardy.

(29) Post false statements, and/or assume the identity of another person.

b. Access and Security Prohibitions

Users must immediately notify the Director of Technology and/or designees, if they have identified a possible security problem. Users must read, understand, and submit an electronically or written signed *CIS Acknowledgment and Consent Form(s)*, and comply with this policy that includes network, Internet usage, Electronic Communications, telecommunications, non-disclosure and physical and information security policies. The following activities related to access to the School District's CIS systems, and information are prohibited:

(1) Misrepresentation (including forgery) of the identity of a sender or source of communication.

(2) Acquiring or attempting to acquire passwords of others. Users are required to use unique strong passwords that comply with the School District's password, authentication, and syntax requirements. Users must not acquire or attempt to acquire User ID and/or passwords of another. Users will be held responsible for the result of any misuse of Users' names or passwords while the Users' systems access were left unattended and accessible to others, whether intentional or, whether through negligence.

(3) Using or attempting to use Computer accounts of others. These actions are illegal, even with consent, even if only for the purpose of "browsing".

(4) Altering a communication originally received from another person or Computer with the intent to deceive.

(5) Using School District resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons. Such acts would include, but not be limited to, as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property.

(6) Disabling or circumventing any School District security, program or device, including, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.

(7) Transmitting Electronic Communications anonymously or under an alias unless specifically authorized by the School District.

(8) Accessing any website that the School District has filtered or blocked as unauthorized. Examples include, but are not limited to, accessing unauthorized social networking, music download, and gaming sites.

(9) Users must protect and secure all electronic resources and information, data and records of the School District from theft and inadvertent disclosure to unauthorized individuals or entities at all times. If any User becomes aware of the improper release of School District information, data or records, the release must be reported to the Superintendent, and/or designee, immediately.

c. Operational Prohibitions

The following operational activities and behaviors are prohibited:

(1) Interference with, infiltration into, or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of Computer "worms" and "viruses", Trojan Horse, trapdoor, robot, spider, crawler, and other program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. The User may not hack or crack the network or others' Computers, whether by spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems or the systems of others, or any component of the network, or strip or harvest

information, or completely take over a person's Computer, or to "look around".

(2) Altering or attempting to alter files, system security software or the systems without authorization.

(3) Unauthorized scanning of the CIS systems for security vulnerabilities.

(4) Attempting to alter any School District computing or networking components (including, but not limited to fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.

(5) Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any Computer, Electronic Communications Systems, or network services, whether wired, wireless, cable, virtual, cloud, or by other means.

(6) Connecting unauthorized hardware and devices to the CIS systems.

(7) Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but is not limited to, downloading music files.

(8) Intentionally damaging or destroying the integrity of the School District's electronic information.

(9) Intentionally destroying the School District's Computer hardware or software.

(10) Intentionally disrupting the use of the CIS systems.

(11) Damaging the School District's Computers, CIS systems, networking equipment through the Users' negligence or deliberate act including but not limited to vandalism.

(12) Failing to comply with requests from appropriate teachers or School District administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

5. Content Guidelines

Information electronically published on the School District's CIS systems shall be subject to the following guidelines:

a. Published documents, including but not limited to audio and video clips or conferences, may not include a student's date of birth, Social Security number, driver's license number, financial information, credit card number, health information, phone number(s), street address or box number, name (other than first name) or the names of other family members, without parental consent.

b. Documents, web pages, Electronic Communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

c. Documents, web pages, Electronic Communications, or videoconferences may not contain objectionable materials or point directly, or indirectly, to objectionable materials.

d. Documents, web pages and Electronic Communications, must conform to all School District policies, regulations, rules, and procedures.

e. Documents to be published on the Internet must be edited and approved by the Director of Technology.

6. Due Process

a. The School District will cooperate with School District, the ISP, and local, state, and federal officials to be reasonably cooperative in investigations concerning or relating to any illegal activities allegedly conducted through the School District's CIS systems.

b. If students or employees are entitled to due process rights for discipline resulting from the violation of this policy, they will be provided such rights.

c. The School District may terminate any account privileges by providing notice to the User(s).

7. Search and Seizure

a. Users' violations of this Policy, any other School District policy, or the law may be discovered by routine maintenance and monitoring of the School District's CIS system, or any method stated in this policy, or pursuant to any legal means.

b. The School District reserves the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, record, check, track, log, access, or otherwise inspect; and/or report all aspects of its CIS systems. This includes items related to any personal Computers, network, Internet, Electronic Communications systems, databases, files, software, and media that individuals bring onto the School District's property, or to School District's events, that were connected to the School District network, and/or that contain School District programs, or School District or Users' data or information, all pursuant to law, in order to insure compliance with this policy, other School District policies, regulations, rules, and procedures in order to protect the School District's resources, and to comply with the law.

c. Any information that users place in their individual files should be entered with the knowledge and understanding that i t is subject to review by a third party.

8. Copyright Infringement and Plagiarism

a. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the School District resources. See School District Copyright Policy #814. Users will make a standard practice of requesting permission from the holders of the work, and complying with the Fair Use Doctrine, and/or complying with license agreements.

b. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The School District does not permit illegal acts pertaining to the copyright law. Therefore, any User violating the copyright law does so at their own risk and assumes all liability.

c. Violations of copyright law include, but are not limited to, making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on or from, the School District's Computers is expressly prohibited. This includes all forms of licensed software - shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.

d. No one may circumvent a Technology Protection Measure that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a Technology Protection Measure to control access to a copyright protected work.

e. School District guidelines on plagiarism will govern use of material accessed through the School District's CIS systems. Users must not plagiarize works that they find. Users understand that use of the School District's systems may involve the School District's use of plagiarism analysis software being applied to their works.

9. Selection of Material

a. School District policies on the selection of materials will govern use of the School District's CIS systems.

b. When using the Internet for class activities, teachers must select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers must preview the materials and websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions About controversial issues while demonstrating tolerance and respect for those who hold divergent views.

10. School District Website

The School District will establish and maintain a Website and will develop and modify its Web pages to present information about the School District under the direction of the Director of Technology and/or designees. Publishers must comply with this policy, other School District policies, regulations, rules, and procedures. The School District may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions.

11. Blogging

a. If an employee, student or Guest creates a blog with their own resources, the employee, student, or Guest may not violate the privacy rights of employees and students, may not use School District personal and private information/data, images

and/or copyrighted material in their blog, and may not disrupt the operations of the School District.

b. Contrary conduct will result in actions further described the "Consequences for Inappropriate, Unauthorized and Illegal Use" section of this policy and as provided in relevant School District policies, regulations, rules, and procedures.

12. Safety and Privacy

a. To the extent legally required, Users of the School District's CIS systems will be protected from harassment or commercially unsolicited Electronic Communications. Any User who receives threatening or unwelcome communications must immediately send or otherwise provide them to the Director of Technology and/or designees.

b. Users will not post personal contact information about themselves or other people on the CIS systems. Users may not steal another's identity in any way, may not use spyware, cookies, or use School District or personal technology or resources in any way to invade another's privacy. Additionally, Users may not disclose, use or disseminate confidential and personal information about students or employees. Examples include, but are not limited to revealing: biometric data, student grades, Social Security numbers, date of birth, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the School District, by using a PDA, iPhone, Blackberry, cell phone (with or without camera/video) and/or other Computer, unless legitimately authorized to do so.

c. If the School District requires that data and information be encrypted, users must use School District authorized encryption to protect their security.

d. Student Users, by their use of the District's CIS Systems, agree not to meet with someone they have met online unless they have parental consent.

13. Consequences for Inappropriate, Unauthorized and Illegal Use

a. General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, regulations, rules, and procedures, or for unlawful use of the CIS systems, may result in loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions, employee suspensions (with or without pay), dismissal, expulsions, breach of contract, and/or legal proceedings. These will be handled on a case-by-case basis. This policy incorporates all other relevant School District policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, copyright, property, curriculum, terroristic threat, vendor access, and harassment policies.

b. Users are responsible for theft of, and damages to, Computers, the network, equipment, Electronic Communications systems, and software resulting from accidental, negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from negligent, willful

or deliberate violations of this policy, related policies, regulations, rules, and procedures. For example, Users will be responsible for payments related to lost or stolen Computers and/or School District equipment, and recovery and/or breach of the data contained on them.

c. Violations as described in this policy, other policies, regulations, rules and procedures may be reported to the School District, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. Actions which constitute a crime under state and/or federal law, could result in arrest, criminal prosecution, and/or lifetime inclusion on a sexual offenders registry The School District will be reasonably cooperative with authorities in all such investigations.

d. Vandalism to CIS Systems will result in cancellation of access to the School District's CIS systems and resources and is subject to discipline.

e. Any and all costs incurred by the School District for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this policy, other School District policies, regulations, rules, and procedures, or federal, state, or local law, must be paid by the User who caused the loss.

G Suite for Education Notice to Parents and Guardians

At Lake-Lehman School District, we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At Lake-Lehman School District, students will use their G Suite accounts to complete assignments, communicate with their teachers, sign into their Chromebooks, and learn 21st century digital citizenship skills.

The notice below provides answers to common questions about what Google can and can't do with your child's personal information, including:

- What personal information does Google collect?
- How does Google use this information?
- Will Google disclose my child's personal information?
- Does Google use student personal information for users in K-12 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will not create or remove a G Suite for Education account for your child. Students who cannot use Google services will need to use other means for completing assignments such as hard copied assignments/tests on paper.

By signing the Lake-Lehman School District Acceptable Use Policy (AUP), I give permission for Lake-Lehman School District to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google (described at https://gsuite.google.com/terms/user_features.html):

- Gmail
- Google+
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
- Jamboard
- Keep
- Sites
- Vault

In addition, we also allow students to access certain other Google services with their G Suite for Education accounts. Specifically, your child will have access to the following "Additional Services":

- YouTube, Blogger, Google Maps, Google Earth, Google Cloud Print, Search and Assistant, Chrome Web Store.

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Lake-Lehman School District may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
- log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in K-12 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- With Lake-Lehman School District. G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in

compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.

- For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting the Director of Technology. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit https://myaccount.google.com while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact Director of Technology. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Center (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html) [if school/district has accepted the Data Processing Amendment (see https://support.google.com/a/answer/2888485?hl=en), insert: and the Data Processing Amendment (at https://www.google.com/intl/en/work/apps/terms/dpa_terms.html)].

Lake-Lehman School District
PO BOX 38
Lehman, PA 18627

Acceptable Use of Communications and Information (CIS) Systems Policy

CIS Acknowledgment and Consent Form

Students

I have received, read, and understand the Acceptable Use of Communications and Information (CIS) Systems Policy, and will comply with it. Someone from the School District has also reviewed this Policy with me and my parents have reviewed it with me. In addition, I have been given the opportunity to obtain information from the School district and my parent(s) about anything I do not understand, and I have received the information I requested. If I have further questions, I will ask the Director of Technology and my parents. Additionally, I understand that if I violate this policy, other related policies, regulations, rules, and procedures, I am subject to the School District's discipline and could be subject to ISP, as well as local, state and federal laws and procedures.

_____

Name of Student Grade Level

_____

Signature of Student Date

Parents(s)

As the parent of a student of the School District, I have received, read, and understand the Acceptable Use of the Communications and Information (CIS) Systems Policy. In addition, I reviewed this Policy with my child and answered questions he or she asked. If either my child or I have further questions, I will ask the Director of Technology. I agree to have my child comply with the requirements of this Policy, other related policies, regulations, rules, and procedures. Additionally, I understand that if (s)he violates this policy, other related policies, regulations, rules, and procedures (s)he is subject to the School District's discipline, ISP requirements, as well as local, state and federal laws and procedures.

_____

Name of Parent

_____

Signature of Parent Date