INTERNET, NETWORK AND EMAIL RESPONSIBLE USE POLICY FOR STAFF

The Children's Internet Protection Act, known as CIPA, became effective on April 20, 2001. According to the FCC, schools and libraries must certify that they are enforcing a policy of Internet Safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. They must also have adopted and implemented an Internet Safety Policy that addresses specific issues. In addition, pursuant to the Protecting Children in the 21st Century Act, the Plainville School District will monitor the online activities of minors and educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms. The district will also educate minors about cyberbullying awareness and potential responses.

The Children's Online Privacy Protection Act (COPPA) was enacted by Congress in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 29, 2012. The amended Rule which took effect on July 1, 2013 spelled out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online. The new rule added four new categories of information to the definition of personal information. Operators are required to obtain parental consent for the following:

- Geolocation information sufficient to identify street name and name of a city or town, regardless of when such data is collected
- Photos or videos containing a child's image or audio files with a child's voice from a child
- Screen or user name is personal information where it functions in the same manner as online contact information
- Persistent identifiers such as information about a child's activities on its website or online service

OVERVIEW

Plainville Technology Mission Statement

We are strongly committed to prepare students to be technologically literate in the skills needed to compete in an information based global community of the 21st century. To ensure this, we must enhance our curriculum to guarantee that technology becomes an integral and routine part of the learning and teaching experience for everyone in the Plainville education system.

In keeping with its mission statement, the goal of the Plainville School District is to promote educational excellence by facilitating resource sharing, innovation and communication, and also by encouraging the safe use of digital tools and Internet resources in a caring learning environment.

The Internet is an electronic communications network that provides vast, diverse and unique resources. Access to the Internet and e-mail allows teachers and staff the opportunity to explore thousands of libraries, databases, museums, and other repositories of information and to exchange personal communications with other Internet users around the world. The Plainville School District views information gathered from the Internet in the same manner as reference materials identified by the schools. Specifically, the district supports resources that will enhance the learning environment with directed guidance from administrators, teachers and staff. Exploration, discovery and manipulation of resources are encouraged. However, with such great potential for education also comes some potential for abuse. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting.

TECHNOLOGY PROTECTION MEASURE

Teachers and staff must understand that the information available on the Internet is not always age appropriate or accurate. The Plainville School District has installed a firewall to protect the network from hackers and has enabled content filtering on all computers to protect against Internet access by adults and minors to visual depictions that are (a) obscene, (b) pornographic or (c) harmful to minors. While the necessary technology protection measures have been taken to protect students from accessing inappropriate material on the Internet, it is impossible to guarantee that students will not accidentally or purposely find material that is not consistent with the educational mission, goals and policies of the school.

Student access to Plainville emails and use of the Internet will be available only through a student account and as such, will be under teacher direction and monitored. Direct supervision is required. The district requires teachers and staff to monitor students when accessing the Internet and evaluate all Internet resources prior to student use. While students may be able to access Internet resources for research that have not been previewed by staff, the students shall be provided with guidelines and a list of resources that support the curriculum. The district will also provide ongoing student instruction that addresses Internet safety, digital citizenship and ethical use of technology as a tool.

When students are using the Internet, the content filtering software cannot be disabled even with parental or teacher permission and supervision. Upon written request a system administrator may disable content filtering software only for adults who are using the school computers for bona fide research or other lawful purposes.

The most important prerequisite is that the user takes full responsibility for his/her own actions. The Plainville School District will not be liable for the actions of anyone connecting to the Internet through our network. All users assume full liability, legal, financial, or otherwise, for their actions. Access, as provided by the Plainville Schools is considered a privilege not a right. With this privilege comes the responsibility of all users to abide by acceptable use practices.

The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully, understand(s) their significance, and will abide by the policies and procedures pertaining to the Staff Acceptable Use Policy.

INTERNET AND NETWORK - TERMS AND CONDITIONS OF USE

PRIVILEGES

The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Each user will be trained in the proper use of the network and the Internet. The school district administrators may periodically conduct Internet searches to investigate if teachers have posted inappropriate materials online. The school district administrators will deem what is inappropriate use based upon the criteria outlined in this policy and their decision is final.

PRIVACY

The system administrators may review files and monitor all computer and Internet activity to maintain system integrity and ensure that users are acting responsibly. Privacy is not guaranteed. Any information stored, accessed, browsed and/or created on the Plainville School District's network and/or systems should not be considered private by the user. This includes, but is not limited to, any and all electronically stored information and electronic files, electronic mail communications, and Internet website history. All aspects of the Plainville School district's network and systems usage by a user is subject to monitoring, the Massachusetts Public Records Law, and legal discovery, as applicable.

Electronic mail and other electronically stored information and electronic files are considered public records subject to potential disclosure under the Massachusetts Public Records Law unless exempted and its record retention policies and may be subject to legal discovery. Employees should therefore NOT expect that electronic mail messages (even those marked "Personal") are private or confidential.

ACCEPTABLE USES

The Plainville School District's network and systems are provided at the expense of the district and are to be used in furtherance of educational purposes. The purpose of the backbone networks making up the Internet is to support research and education in and among the academic institutions by providing access to unique resources and the opportunity for collaborative work. Access must be consistent with the educational objectives of the Plainville School District. Use of other organizations' network or computing resources must comply with the rules appropriate for those networks.

UNACCEPTABLE USES

Certain activities and behaviors are not permitted. These include, but are not limited to:

- Unauthorized access, including so called "hacking" and illegal activities are strictly forbidden.
- Unauthorized disclosure, use, and dissemination of personally identifiable information is prohibited
- Access to inappropriate material on the Internet is prohibited.
- Transmission of any material in violation of any national or state regulation is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material or material protected by trade secrets.
- Use of the Internet for commercial activities, product advertisement or political lobbying is prohibited.

SCHOOL APPROVED DEVICES

The Plainville School District may provide staff members with school approved devices to promote learning outside of the classroom. Staff members are expected to abide by the same responsible use policy when using school approved devices off the school network as on the school network. Use of school-issued devices off the school network may be monitored.

Staff members are expected to use them for educational purposes that are school-related in the performance of job duties unless otherwise explicitly authorized by Administration. They are to treat them with extreme care and caution, and are prohibited from loaning them to another staff member, student or family member. The person to whom the device is issued will be responsible for any activity or action performed on the device. The device configuration shall not be altered in any way by staff members and must be returned in acceptable working order by the last day of each school year, upon withdrawal or exit date from the school district, and/or upon request for maintenance and updates. Staff members are expected to report any loss, damage, or malfunction to the IT Department immediately. Staff members may be financially accountable for any damage resulting from negligence or misuse. In such instances an administrative investigation will be conducted prior to a staff member being held financially responsible.

PERSONALLY OWNED ELECTRONIC DEVICES (POEDs)

Staff members may bring into the school district their POEDs such as cell/smart phones, laptops, notebooks and tablets for teaching and learning, professional development and job-related activities. They must not use their POEDs to harass or victimize other students or staff, or to abuse a person's right to privacy. Student related information must not be stored on POEDs unless they receive parental written notice and consent. At the end of each school year, any student related information will be deleted from the POEDs. POEDs are the sole responsibility of the device owner and must adhere to the following guidelines:

- The devices should be password protected for security purposes
- The devices should have the latest Virus Protection software including the latest virus definition files.
- The devices should have the latest Security Patches for its operating systems.
- The devices should be free of spyware, adware, worms, viruses, trojan horses, and peer to peer software that could disrupt the network.
- The devices should not be used for any illegal activity, peer-to-peer file sharing (including Kazaa, Limewire, Gnutella, Napster, Bit Torrent, etc.,) or unauthorized access to any device.
- The devices should not have Internet Connection Sharing services turned on.

The Plainville School District will not be held responsible for the loss, theft or destruction of any POEDs. The Plainville School District will not provide technical support or assume any responsibility for loss or damage of any software, hardware or data on any POEDs. Should inappropriate activities or a security breach be detected, system administrators may examine the POEDs. In using their POEDs, staff members are expected to comply with the Responsible Use Agreement for Staff.

ACCESS TO WIRELESS NETWORK

The Plainville School District will provide a filtered, wireless network to which staff members will be able to connect personally owned electronic devices (POEDs) for instructional and administrative functions. To connect to the school district wireless network, staff members must register their personally owned electronic devices (POEDs) with the School District IT Department. Plainville School District will not be held responsible for use of any information obtained via the wireless network including but not limited to loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors, and/or omissions. Users are not to disrupt the use of the wireless network. Use of the wireless network is at the user's own risk.

VIDEO CONFERENCING

Videoconferencing such as Skype is a way that users can communicate with other users, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, users can see, hear, and speak with other users, speakers, museum personnel, etc. in real-time. Videoconference sessions may be videotaped by district personnel or by a participating school involved in the exchange in order to share the experience within their building or school district. Users' voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session. Rules and procedures relative to responsible use and behavior by users apply during all videoconferencing sessions.

DATA CONFIDENTIALITY

The efficient collection, analysis, and storage of student information is essential to improving the education of our students. As the use of student data has increased and technology has advanced, the need to exercise care in the handling of confidential student information has intensified. It is the responsibility of all staff to use appropriate judgment and extreme caution when accessing all confidential and sensitive electronic information. This information includes staff and student personally identifiable data that is stored on the local network and through school approved online services such as Schoolbrains, Illuminate, One Drive and SharePoint.

Confidential information includes any information or data that can identify a particular student. This includes not only the student's full name, but also the student's ID number, social security number, any unique logins associated with a particular student, photos, videos, geolocation data, the IP address of the student's computer, or unique identifiers associated with a mobile device belonging to the student.

All staff are strictly prohibited from disseminating such confidential information outside of the Plainville Schools local network or online services unless authorized by Administration and/or required by their jobs. When sharing sensitive and/or confidential documents through One Drive and SharePoint, staff must place a check next to "Require Sign-in" option whenever available.

All staff are advised to review the pre-approved list of online educational resources on the school website. Any online educational resources that require the setup of class rosters must be properly vetted by the district to ensure compliance with COPPA (Children's Online Protection and Privacy Act). Staff should provide minimal student information such as their first name followed by first initial of their last name unless they are exported directly from our Student Information System. All staff must safeguard electronic student data privacy in order to be in compliance with the Family Education Rights and Privacy Act (FERPA), Massachusetts student record regulations, 603 C.M.R. 23.00 ("State Regulations") and COPPA (Children's Online Privacy and Protection Act).

NETWORK ETIQUETTE

Staff members are expected to abide by the accepted rules of network etiquette. These include, but not limited to, the following:

- Be polite. Do not get abusive in your messages to others.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- Do not disrupt the use of the network.

LIABILITIES

The Plainville School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. Plainville School District will not be responsible for any damages the user suffers including: loss of data resulting from delays, miss-deliveries or service interruptions caused by network disruptions or user errors or omissions. Use of information via Internet is at the users' own risk. The Plainville School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

SECURITY

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a system administrator. Do not demonstrate the problem to other users. Do not use another individual's account without written permission from that individual. Attempts to logon to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.

VANDALISM

Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks that are connected to any of the Internet backbones. This includes, but is not limited to, the uploading or creation of computer viruses.

ELECTRONIC MAIL (E-MAIL)

PURPOSE

The purpose of the e-mail policy is to ensure proper use of the Plainville School District's e-mail system and to support business and educational functions. The Plainville School provides the e-mail system as a means of communication to further education, research and the mission of the school district and must be regarded as public documents. All personnel who use the e-mail system are required to comply with the following guidelines.

NO RIGHT TO PRIVACY

Any computer files or electronic mail ("e-mail") messages maintained, stored, received or sent on or from the Plainville Public School ("the District") computer systems are and shall remain property of the District and are subject to being monitored and/or disclosed at any time by the District. All employees have no privacy interests in e-mail messages or passwords, and as a condition of the use of the District's system, consent to the District's monitoring and disclosure of e-mail messages.

Subject to certain exceptions in the law, email and other electronically stored information and electronic files are considered public records subject to potential disclosure under the Massachusetts Public Records Law and its record retention policies and may be subject to legal discovery. Employees should NOT expect that email messages (even those marked "Personal") are private or confidential.

MONITOR

The Plainville School District reserves the right to monitor, access, and review any e-mails or other materials transmitted by the senders and recipients, at any time, without prior notice, by authorized personnel. This is to ensure that there are no violations of the law, breaches of company policies and any communications that may be harmful to the school district, or for any other reason. Users of the Plainville School District email system consent that the monitoring identified in this policy shall not constitute an invasion of his or her privacy.

GENERAL RESTRICTIONS ON CONTENT OF E-MAIL MESSAGES

The e-mail system has been installed by the district for use in the conduct of district business. The district recognizes, however, that employees may desire to use the e-mail system occasionally for personal purposes. The district will permit such occasional, personal use of the e-mail system, provided that:

- such use does not result in additional cost to the district;
- such use is not over used or abused by employees; and

- employees understand (and are hereby informed) that all messages transmitted or received on the e-mail system, of whatsoever nature, remain fully subject to all the provisions of this e-mail policy (thus, for example, even personal messages on the e-mail system constitute district property in which employees have no right of privacy and which may be stored, monitored, or disclosed at any time by the district).

The e-mail system shall not be used to transmit messages, either within the district or in communications transmitted outside of the district, that might reflect poorly on the district, including language that may be construed as harassment or disparagement of others based upon their race, color, national origin, sex, sexual orientation, age, marital or familial status, physical or mental disability, or religious or political beliefs.

PERIODIC DELETION OF E-MAIL MESSAGES

E-mail, electronic files, and other electronically stored information concerning official Plainville School District business are generally considered "public records" that are subject to disclosure under the Massachusetts Public records Law, unless an exemption applies. (M.G.L. c. 66. § 10: M.G.L. c. 4, s. 7(26).

Public Records include all "books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any officer of employee..." of the district, unless such matters are exempt from disclosure under the Massachusetts Public Records Law. (M.G.L. c. 4, s. 7(26).

E-mail messages may be printed and filed in accordance with existing public record filing procedures and retention standards. However, e-mail and other electronically stored information should be retained in an electronic format as required by the Massachusetts Public Records Law. Please consult the Public Records Division of the Office of the Secretary of the Commonwealth for details regarding how this law affects your particular file, document, e-mail message or record.

OFFENSIVE OR HARASSING PROHIBITED

The e-mail system must not be used to create any offensive or disruptive messages. Among those which are considered offensive, are messages or materials which contain sexual references or implications, racial or ethnic slurs, or other comments that offensively address someone's age, sex, sexual orientation, religion, national origin, ancestry or disability. In addition, the e-mail system must not be used to communicate other improper messages or images that are defamatory, derogatory, obscene or otherwise inappropriate. The e-mail system must not be used to commit any crime, including but not limited to sending obscene e-mails or images with the intent to annoy, abuse, threaten, or harass another person.

SOLICITATION PROHIBITED

The e-mail system may not be used to solicit outside, personal or commercial ventures, religious or political causes or other solicitations that are not work related.

PROHIBITED USES

The e-mail system must be used appropriately, responsibly, and in a lawful manner. This includes not sending or forwarding unsolicited e-mails such as "chain" e-mail letters, junk e-mail (spam) and daily jokes; forging or attempting to forge e-mails and sending an e-mail using another person's e-mail account.

PROTECTING THE CONFIDENTIALITY OF PROPRIETARY INFORMATION

Employees should be aware that communications on the e-mail system may potentially be accessed and reviewed by persons other than the intended recipient. When transmitting sensitive or privileged information, employees should always use the most secure form of transmission that is available to them and that ensures the safety and security of the information being transmitted. In the event that e-mail is used to transmit sensitive or privileged information, employees should take all reasonable steps to ensure that the information is as secure as possible, preferably, through the use of e-mail that is encrypted or password-protected, if such technology is available. When transmitting e-mails that contain student information, employees must use student's initials, not their first or last name. Employees shall promptly notify the superintendent's office in the event an e-mail transmission containing confidential or proprietary information of another party is received without the express permission of that party.

E-MAIL ETIQUETTE

- Check your e-mail regularly, at least once a day. E-mail is generally expected to be replied within 48 hours; if the e-mail is complicated, do send an e-mail acknowledging the receipt of the e-mail and that you will get back to the person soon.
- Be concise and to the point – e-mail can be discouraging to read if it is too long.
- Always use informative, short and carefully phrased subject title to reference the e-mail. Do not leave the subject title blank.
- Do not use the e-mail system to communicate any sensitive or confidential information. It is not secure. E-mails can be intercepted by others.
- Do not use the e-mail system if there is a chance your message can be misunderstood. If the situation is complex and can be misinterpreted, use the phone or arrange for a personal meeting instead.
- Be careful when using the Reply or Reply to All in response to e-mails.
- Do not use capital letters – if you write in CAPITAL LETTERS, the recipient may interpret it as shouting and treat the e-mail as annoying and may not reply.
- Read your e-mail before sending – check for spelling mistakes. This will avoid any misunderstandings or unnecessary comments.
- Do not open an e-mail or attachment if you do not know the sender. Please delete it immediately. We must take precautions to prevent any unknown viruses that may have come through the e-mail system.

PURCHASE AND INSTALLATION OF SOFTWARE

- Unauthorized download and installation of any software without prior written approval of the system administrators is prohibited.
- Do not purchase any personal software for the computers in your classrooms.
- Software that was not purchased by the school should not be installed on the computers in school.
- Software that was originally purchased for your home computer should not be installed on the computers in school.
- Software will be used in accordance with its license agreement. Software that has a single user license cannot be installed on multiple computers unless otherwise noted in the license agreement. Unless otherwise noted, all software and files (audio, pictures, photos, text) on the Internet should be considered copyrighted work. Do not download software and/or files without the permission of the copyright holders

VIOLATION OF POLICY

When inappropriate use of computers and websites is discovered, the school district administrators will promptly bring that inappropriate use to the attention of the staff member. The school district administrators may close an account or deny access any time as required, and may consider disciplinary action up to and including termination of employment.