RULES AND REGULATIONS
IMPLEMENTING BOARD POLICY 6:235

ACCESS TO ELECTRONIC NETWORKS

I. Scope of Rules and Regulations and School District Authority

These Rules and Regulations are promulgated pursuant to the Access to Electronic Networks Policy (the "Policy"). These Rules and Regulations govern all use of District computers including Mobile Devices, the District's local and/or wide area network, and all access to the Internet through District computers or any Mobile Device whether or not District-owned, or the District's local and/or wide area network, which will be collectively referred to in these Rules and Regulations as the District's "Network." A "Mobile Device" is any electronic device that has the capability of accessing the Internet, whether through wireless connection or other means.

The Policy and these Rules and Regulations may be supplemented by additional rules, regulations, and other terms and conditions of computer network use that may be promulgated by District staff pursuant to the Policy or these Rules and Regulations.

The goal of the Board is to include appropriate Network access in the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. All use of the Network shall conform to the requirements of all District policies

II. Obtaining Authorization to Use Network

A. Authorized Users

Authorized users of the Network include students, teachers, administrators, other employees of the District, and Board of Education members who have been given access to the Network, have submitted the appropriate authorization forms, and whose Network privileges are not suspended or revoked.

B. Students

1. Access of Network through District-Owned Devices. To obtain access to the Network through a District-owned computer or District-owned Mobile Device, a student must submit a properly signed copy of the Student and Parental Authorization for Electronic Network Access form (Exhibit 1, the "Network Authorization") to a designated District employee.

2. Access of Network through Personal Mobile Devices. The District recognizes the value technology can bring to the students' educational experiences. At times, it may be helpful to student learning for personal Mobile

Devices to be used at school. With parent consent and student understanding of the Policy and these rules and regulations, a student may use, with teacher permission, a personal Mobile Device to access the Network for educational purposes. In such cases, the student must utilize the District's guest wireless network and turn off any private network. By doing so, the student will have access to a filtered Internet in compliance with the Policy and these rules and regulations. In addition, the student will only use appropriate educational applications on their personal Mobile Devices.

During school hours and/or on District property, students are prohibited from using their district or personal Mobile Device: (1) to access private networks or bypass or attempt to bypass the District's guest wireless network; (2) to call, text message, email, or otherwise electronically communicate with others, including students, parents/guardians, friends and families, without teacher pre-approval; (3) to record audio or video media or take pictures of any student or staff member without teacher pre-approval; (4) to distribute any unauthorized media; (5) in locker rooms and washrooms; (6) for any unacceptable use as set forth in the Policy and these rules and regulations; and (7) in any manner that violates any Board policy, rule or Code of Conduct.

The student is responsible for setting up and maintaining his/her personal Mobile Device, including ensuring that the Mobile Device has virus protection and is free of any viruses or other files that may affect the Network. The District is not responsible for providing technical support to students who utilize a personal Mobile Device.

The student is also responsible for the safety and security of his/her Mobile Device. The District is not responsible for the safety, security or loss of, or damage to a student's personal Mobile Device.

The District may inspect and search the contents of a personal Mobile Device on school property if there is reasonable suspicion to believe that the Mobile Device was used in violation of school policies or rules or the law. A student may be subject to discipline for violating the rules regarding the use of personal Mobile Devices, up to and including expulsion.

To obtain access to the Network through a personally-owned Mobile Device, a student must submit both the Network Authorization and a properly signed copy of the Student and Parental Authorization for Personal Mobile Device Use form to a designated District employee.

3. Maintenance and Completion of Authorization Forms. A record of the student's submission of these forms will be kept in the student database. Copies of these forms or electronic backups shall be kept at the school which the student attends.

Students and parents/guardians must complete and submit a Network Authorization form (online or on paper) and a Personal Mobile Device Authorization form, if applicable, at the beginning of each school year. Upon submission of the newly-signed form(s), the District will renew the student's access to the Network.

Unless a student's Network privileges have been suspended or revoked, the Network Authorization form and Personal Mobile Device Authorization form, if applicable, will authorize that student's access to the Network for that school year. If a student's Network privileges are suspended or revoked, a newly-signed copy of the Network Authorization form and the Personal Mobile Device Authorization form, if applicable, must be submitted before the student's access privileges are restored.

4. Disciplinary Consequences. Any violation of the terms of these forms, the Policy, these Rules and Regulations, or additional rules, regulations or other terms and conditions of Network access promulgated by the Superintendent or Building Principals may result in the suspension or revocation of Network privileges, disciplinary action, and/or appropriate legal action.

C. Non-Student Users

To obtain Network access via a District-owned computer or any Mobile Device, teachers, other District staff members, volunteers and Board members ("Non-Student Users") must submit a signed copy of the Non-Student Authorization for Electronic Access form (Exhibit 3, "Non-Student Authorization").

A Non-Student User must complete the Non-Student Authorization form at the beginning of each school year. Upon submission of the newly-signed form, the District will renew the Non-Student User's access to the Network. If a Non-Student User's Network privileges are suspended or revoked, the user must submit a newly-signed Non-Student Authorization form before the user's access privileges are restored.

Any violation of the terms of this form, the Policy, these Rules and Regulations, or additional rules, regulations or other terms or conditions of Network access promulgated by the Superintendent or Building Principals may result in the suspension or revocation of Network privileges, disciplinary action, and/or appropriate legal action.

III. Use of Computer Network

A. Acceptable Use

1. Curriculum Purposes. Access to the Network is limited to bona fide educational or research purposes consistent with the District's educational mission. Access also must comply with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of computer network access promulgated by the Superintendent, Executive Director of Educational Technology, or Building Principals, and all other disciplinary policies and regulations necessary for the safety and pedagogical concerns of the District.

2. General Use by Employees. Employees may access the Network for personal use during times when the employee is not instructing, supervising students, or otherwise performing responsibilities related to their job duties (e.g., parent-teacher conferences, in-services, IEP meetings, etc.) and when such use is not negatively impacting the employee's work duties and performance, interfering with the operations of the District, or violating the rights of others. Such personal use must be reasonable, professional and appropriate at all times. District employees are representatives of the District and have a duty to act in a professional manner while using the Network.

B. Unacceptable Use

Any use which: (1) disrupts the proper and orderly operation and discipline of schools in the District; (2) threatens the integrity or efficient operation of the Network; (3) violates the rights of others; (4) is socially inappropriate or inappropriate for a student's age or maturity level; (5) is primarily intended as an immediate solicitation of funds; (6) is illegal or for illegal purposes of any kind; (7) violates any Board policy, rule or procedure; or (8) constitutes gross disobedience or misconduct is an unacceptable use. Use of the Network for any unacceptable use may result in the suspension or revocation of Network privileges, disciplinary action up to and including expulsion (for students) or termination from employment (for employees), and/or appropriate legal action.

Unacceptable uses of the Network specifically include, but are not limited to, the following:

1. Taking any steps which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building, or property with harm, regardless of whether the user intends to carry out such threat, including cyber-bullying. (Cyber-bullying is defined as, but is not limited to, harassing, teasing, intimidating, threatening or terrorizing another person by sending or posting inappropriate and harmful email messages,

instant messages, text messages, digital pictures, images or video, or web site postings via social networking sites or other electronic means.);

2. Compromising the privacy or safety of other individuals by disclosing personal addresses, telephone numbers, or other personal identifying information without that person's permission;

3. Accessing, using or possessing any material in a manner that constitutes or furthers fraud (including academic fraud), libel, slander, plagiarism, forgery, or a violation of copyright or other intellectual property right or transmitting any material in violation of State or Federal law;

4. Using the Network for commercial, private, or personal financial gain, including gambling;

5. Deliberately accessing, creating, submitting, posting, publishing, transmitting, receiving, displaying, or otherwise possessing or disseminating any material that is defamatory, abusive, obscene, profane, sexually oriented, sexually explicit, perversely lewd and vulgar, threatening, harassing or illegal, including indecent or inappropriate language, text, sounds, or images;

6. Creating or forwarding chain letters, "spam," or other unsolicited or unwanted messages;

7. Gaining unauthorized access to resources or entities, including, but not limited to, other student files, teacher files, confidential information, student record data, and unauthorized computer network accounts;

8. Coercing or sending email or other communications which purport to come from another individual (commonly known as "spoofing"), or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses or organizations;

9. Modifying, disabling, compromising, or otherwise circumventing any anti-virus, user authentication, or other security feature maintained on the Network or on any Mobile Device, external computer, computer system, or computer account;

10. Using or accessing another user's Network account or password, with or without consent from the user;

11. Downloading or installing text files, images, or other files to the Network without prior permission from the Superintendent, Executive Director of Educational Technology, Building Principal, or their designees;

12. Downloading, installing, or updating software to the Network without prior permission from the Superintendent, Executive Director of Educational Technology, Building Principal, or their designees (Staff requesting the installation of software need to submit the appropriate form to their Technology Facilitator.);

13. Creating or deliberately downloading, uploading, or forwarding any computer virus, or otherwise attempting to modify, destroy, or corrupt computer files maintained by any individual on the Network, any computer, or any Mobile Device;

14. Participating in, or subscribing to non school-related mailing lists, newsgroups, chat services, electronic bulletin boards, or any other non-school related association or service through the Network;

15. Students using encryption software or otherwise encoding or password-protecting any file which is created with, sent to, received by, or stored on the Network;

16. Using the Network for the purpose of harassing other users or other individuals;

17. For Non-Student Users, using the Network to participate in acts constituting "prohibited political activities" under the *State Officials and Employees Ethics Act* or "election interference" under the *Election Code*, or to participate in any political activities that create the appearance of impropriety under those laws or under any ethics policy of the District relating to political activities of District employees;

18. Using the Network resources, such as file space, in a wasteful manner;

19. For Employees, failure to abide by Board Policy 5:125, *Electronic Communication & Social Networking*, and its implementing Guidelines/Procedures;

20. For Employees, personal use of the Network which negatively impacts that employee's work performance or duties, interferes with the operations of the District, or violates the rights of others;

21. For Students, using the Network in a manner that violates any provision of the Board's Discipline Policy or Student Code of Conduct;

22. Attempting to commit any action which would constitute an unacceptable use if accomplished successfully.

IV. Student Use of the Network and Internet

A. Procedures

Students shall abide by the rules, regulations and procedures implemented by this Policy and their teachers when using the Network at school.

Student access to the Internet is allowed only under the direct supervision of a teacher for a specific educational purpose or as otherwise allowed under Board Policy or the One-to-One District iPad Initiative.

B. Internet Safety

The District's primary concern in maintaining Internet access is that student safety and security may not be compromised at any time. Some of the most effective safety measures can only be implemented by students themselves. The District strongly recommends parents/guardians discuss the following safety concerns with their children:

1. Students should never give out such personal information as their name, age, home address, telephone number(s), photograph, their parents'/guardians' work address or telephone number, or the name or location of the school over the Internet or through email. Students should never give out such personal information about other individuals over the Internet or through email.

2. Students should immediately inform their parents/guardians, or a member of District staff it they come across any information on the Internet, in an email or via any other electronic communication that makes them feel uncomfortable. Students should not respond to any such email or other message.

3. Students should never agree to meet someone in person whom they have "met" online without parental knowledge, permission, and supervision.

4. Students should never agree to send or accept any item to or from a person whom they have "met" online without parental knowledge, permission, and supervision.

V. Downloads

Users may only download text files, images, or other files or software obtained through the Internet, e-mail, file transfer protocol (ftp), or other means of file-sharing on the Network with the permission of the Superintendent, Executive Director of Educational Technology, Building Principal, or their designees.

VI. Privacy

Any electronic communications or files created on, stored on, or sent to, from, or via the Network, whether on District-owned or personally-owned computers or any Mobile Device, are the property of the District. Consequently, users do not have any expectation of privacy with respect to such messages and files. Users should remember that such messages and files can be recovered from the Network's backup system even after they have been deleted from a user's individual account.

Each person should use the same degree of care in drafting an electronic mail message as would be put into a written document or memorandum. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.

The Superintendent, Executive Director of Educational Technology, Building Principals, and/or their designees may access and review such messages and files when necessary to maintain the integrity and efficient operation of the Network; to monitor compliance with the Policy, these Rules and Regulations, and all other rules, regulations, or terms or conditions of computer network access promulgated by the Superintendent or designee; and to further all other educational, safety and pedagogical concerns of the District. The District also reserves the right to intercept, access, and disclose to appropriate authorities all information created with, sent to, received by, or stored on the Network at any time, with or without user notice. Use of the Network to create, store, send, receive, view, or access any electronic communication or other file constitutes consent by the user for the District to access and review such files consistent with this paragraph.

Email accounts which are issued by the District to any user remain the property of the District, and the District reserves the right to disclose the email addresses of accounts issued to Non-Student Users to parents and other members of the public consistent with legitimate District purposes.

VII. Technology Protection Measures

Consistent with the District's legitimate educational and pedagogical concerns, the District shall implement technology protection measures, which may include filtering and/or blocking software, on every District computer and Mobile Device which has access to the Internet. Such technology protection measures shall be implemented in the best manner practicable to prevent access to any material, including visual depictions, which is obscene; which constitutes pornography, including child pornography, or which, with respect to use of computers by minors, would be harmful to minors, as defined by the *Children's Internet Protection Act*. The Superintendent, Executive Director of

Educational Technology, Building Principals, or their designees may disable the technology protection measure on an individual computer during use by non-student adults to enable access to material needed for bona fide research or other lawful purpose.

The District shall monitor the use of the Network by employees, students and any other minor user in order to ensure compliance with the Policy, these Rules and Regulations, other rules, regulations or other terms of conditions of Network access promulgated by the Superintendent or Building Principals, and other disciplinary policies and regulations necessary to further the educational, safety, and pedagogical concerns of the District.

VIII. Security

The security and integrity of the Network is a high priority. Users are to keep their account and password secure and confidential at all times. If a Student or Non-Student User believes at any time that he or she has identified a security gap, weakness, or breach on the District's computer network or on the Internet, the user must notify a District staff member immediately. The user may not exploit the gap, weakness, or breach, and the user may not inform any other individuals of it.

Any user who violates this procedure may be subject to a suspension or revocation of computer network privileges, disciplinary action, and/or appropriate legal action.

IX. No Warranties

A. The District makes no warranties of any kind, whether express or implied, for the service of providing Network access to its users, and bears no responsibility for the accuracy or quality of information or services obtained from the Network or any loss of data suffered in connection with use of the Network. The District will not be responsible for any damages any user suffers, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions. Use of any information obtained from the Network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the Network.

B. The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs, relating to, or arising out of, an individual user's use of the Network.

C. The District has acted in good faith and in a reasonable manner in selecting and implementing filtering software, blocking software, and other technology protection measures to prevent access to material which is obscene, pornographic, or, with respect to use of computers by minors, harmful to minors. Nevertheless, by using the Network, users acknowledge that such technology measures do not prevent access to all prohibited material, and may prevent access to non-

prohibited material. The District assumes no responsibility for access gained or denied by the technology protection measures that have been implemented.

X. Indemnification

The user agrees to indemnify the District for any losses, costs, damages, charges or fees, including, but not limited to, telephone charges, long-distance charges, per-minute surcharges, equipment or line costs, or attorney fees, incurred by the District and relating to, or arising out of the user's use of the District's computer network or any violation by the user of the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of Network access promulgated by the Superintendent or designee.

XI. Cooperation with Investigations

The District reserves the right to participate and cooperate fully in any investigation requested or undertaken by either law enforcement authorities or a party alleging to have been harmed by the use of the Network. Evidence of illegal activity shall be reported or turned over to appropriate authorities.

XII. Enforcement

The failure of any user to abide by the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of Network access promulgated by the Superintendent or Building Principals may result in the suspension or revocation of the user's computer network privileges, disciplinary action, and/or appropriate legal action. Computer network privileges may be suspended or revoked by the Superintendent or Building Principal. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies. Discipline may include dismissal for Non-Student Users or expulsion for Student Users.

XIII. Policy Modifications

The Board of Education or its designee may modify the terms and conditions of use and/or the provisions of this Policy and its' implementing Rules and Regulations at any time. The Superintendent or Building Principals may also promulgate additional rules, regulations, or other terms or conditions of computer network access as may be necessary to ensure the safe, proper, and efficient operation of the computer network and the individual District schools. Notice of any such modifications or additional rules, regulations, or other terms or conditions of access shall be promptly communicated to all authorized users, including by posting such modifications on the Network or in a conspicuous place at access locations. Use of the Network constitutes acceptance of the terms of the Policy, these Rules and Regulations, and any additional rules, regulations, or other terms or conditions of computer network access which may have been promulgated by the Superintendent, Building Principals, or their designees.

Exhibit 1

Student and Parental Authorization for Electronic Network Access

To be read and agreed to by Student:

I have read, or have had explained to me, the attached Policy and procedures regarding the use of the School District's electronic network, and I agree that I will follow these rules when I use the District's electronic network. I understand that, if I use the District's electronic network in a way that violates these rules, I can be disciplined. Discipline may include loss of electronic network use privileges, detention, suspension, expulsion or other consequences. I understand that any information, documents, or communication I create or place on the District computer network or send or receive via e-mail or through the Network belong to the District and may be looked at by District employees or others at any time, and that such information or documents will not be private in any way. I know that information or documents placed on the system also may be lost or damaged. I understand that if I misuse the electronic network or cause harm to the Network or anyone else or their information or documents, I may be subject to discipline, and my parents/guardians and I will be responsible for paying for such misuse or damage. By signing below, I demonstrate that I understand and agree to the attached Policy and procedures.

Students are required to have a parent/guardian read and agree to the following:

I have read this and accept the District's *Access to Electronic Networks* Policy and its' implementing Rules and Regulations. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I realize that my child might access objectionable material through the Internet. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting.

I understand that any unacceptable use of the computer network is grounds for suspending or revoking my child's computer network privileges, and may result in disciplinary action against my child, up to and including expulsion from school, as well as criminal or civil penalties.

I agree to indemnify the District and be liable for any losses, costs, damages, charges or fees, caused or incurred by my child relating to, or arising out of, my child's use of the District's electronic network or the violation of any District policy, rules, or regulations. I request that the District allow my child to access the computer network, and agree to hold harmless the Board of Education, its individual Board Members, employees, agents, and assigns, for any harm caused to my student or to me relating to, or arising out of, my student's use of the District computer network or the violation of any District policy.

I have discussed the terms of this *Network Authorization* and the applicable District policy and procedures with my child. I hereby request that my child be allowed access to the District's Internet.

Parent/Guardian Name (*please print*)

Parent/Guardian Signature Date

_____

Student Name (*please print*)

_____ _____

Student Signature Date

Exhibit 2

Teacher and Non-Student Authorization For Electronic Network Access

I, the undersigned, certify that I have read the attached Policy and Rules and Regulations regarding the use of the District's computer network and agree to abide by its terms and conditions. I understand that any unacceptable use shall be grounds for the suspension or revocation of Network privileges; may result in additional discipline up to and including dismissal; and may result in criminal or civil penalties. I understand that the District makes no warranties of any kind, whether express or implied, regarding the Network, and bears no responsibility for the accuracy or quality of information or services obtained from the Network or any loss of data suffered in connection with use of the Network. I agree that all electronic files, including electronic communications, that are created on, stored on, or sent to, from, or via the computer network, whether through District-owned computers or any Mobile Device, are the property of the District; that I do not have any privacy interest in any such electronic files, and that the District may access and review such files consistent with Section VI of the attached Rules and Regulations.

In addition, I agree to indemnify the District for any losses, costs, damages, charges, or fees, including, but not limited to, telephone charges, long-distance charges, per-minute surcharges, equipment or line costs, or attorney fees, incurred by the District and relating to, or arising out of, my use of the District's computer network or any violation of the Policy, Rules and Regulations, or other rules, regulations or other terms or conditions of computer network access promulgated by the Superintendent or Building Principals. In consideration for use of the District's computer network, I hereby release the Board of Education of Glenview School District #34 and its individual Board members, employees, agents and assigns from any claims and damages arising from my use of, or inability to use, the District's computer network.

Name: Signed:

Title: Date:

Exhibit 3 – Only Used on a Case-By-Case Basis

Personal Mobile Device Authorization

To be read and agreed to by Student:

I have read, or have had explained to me, the attached Policy and procedures regarding the use of my personal Mobile Device to access and use the District's Network. I agree to follow these rules when I use a personal Mobile Device. I understand that, if I use a personal Mobile Device in a way that violates these rules, I can be disciplined. Discipline may include loss of use privileges of my Mobile Device, detention, suspension, expulsion or other consequences. I understand that any information, documents or communication created, sent or received via a personal Mobile Device are not private and may be looked at by District employees or others at any time. I further understand that I am responsible for the safety and security of, as well as the setting up and maintenance of, my Mobile Device. By signing below, I demonstrate that I understand and agree to the attached Policy and procedures.

Students are required to have a parent/guardian read and agree to the following:

I have read this and accept the District's *Access to Electronic Networks* Policy and its' implementing Rules and Regulations in regard to my child's use of a personal Mobile Device at school. I understand that in such a situation, my child will use his/her Mobile Device to only access the District's secured wireless guest network, not a private network. I understand that any unacceptable use of the personal Mobile Device is grounds for confiscating and/or suspending or revoking my child's privileges for use of the Mobile Device, and may result in discipline up to and including expulsion from school, as well as criminal or civil penalties. I further understand that my child is responsible for the safety and security of his/her Mobile Device, as well as for the setting up and maintenance of the Mobile Device. I have discussed the terms of this *Authorization* and the District policy and procedures with my child. I hereby give permission for my child to use a personal Mobile Device.

Parent/Guardian Name (*please print*)

Parent/Guardian Signature Date

_____

Student Name (*please print*)

_____ _____

Student Signature Date