GATEWAY REGIONAL SCHOOL DISTRICT
ELECTRONIC COMMUNICATION DEVICES, NETWORK & INTERNET ACCEPTABLE USE POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district Electronic Communication Devices (ECDs) network system, acceptable use of the Internet, and use of Electronic Communication Devices (ECDs).

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student access to the school ECD network system and to the Internet, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district ECD network system and to the Internet enables students to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the ECD network system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

Increased use of school and personal electronic communication devices (ECDs) has both positive and negative consequences. ECDs facilitate student free speech, and schools have incorporated them in teaching and learning with much success. However, student ECD use on and off campus can be abused in a way that negatively affects students, teachers, and the school environment. This policy is intended to support the benefits of ECD use while curtailing possible abuses. The school committee recognizes that all students enrolled in the public school system have the right to attend classes on school campuses that are safe, secure, and peaceful. Acts of bullying, cyberbullying, and sexting are distracting and potential forms of mistreatment that disrupt both a student's ability to learn and a school's ability to educate its students in a safe environment.

The school district, through its school administrators and their designees, has the authority to impose regulations on the possession or use of any ECD while students are on campus, while attending school-sponsored activities, or while under the control or supervision of school district personnel.

Massachusetts sets forth student discipline rules incorporating these policy provisions, defines specific terms such as bullying, cyberbullying and harassment, and describes the circumstances when they are grounds for discipline. (Refer to GRSD bullying policy and bullying plan)

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to school-owned ECDs and the school district's ECD network system, which includes Internet access. The purpose of the system is not merely to provide students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, professional or career development, and limited high quality, self-discovery activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses, which might be acceptable on a user's private personal account on another system, may not be acceptable on this limited purpose network.

During personal time (i.e., during lunchtime, before and after school) in which staff or students have no specific responsibilities to the district, the Internet may be accessed through the District's ECD network for non-professional and personal interests provided that they fall within the realm of the district's "Internet Acceptable Use Policy."

IV. **USE OF SYSTEM IS A PRIVILEGE**

The use of school-owned ECDs, the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of school-owned ECDs, school district systems or the Internet may result in one or more of the following consequences: suspension or cancellation of use of access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws. Law Enforcement may be contacted when school officials reasonably believe a student's communication constitutes a threat to the safety and welfare of members of the school community or where such action may hold the individual criminally liable.

V. **BULLYING AND CYBER-BULLYING**

a. Bullying is prohibited: (i) on school grounds, property immediately adjacent to school grounds, at a school-sponsored or school-related activity, function or program whether on or off school grounds, at a school bus stop, on a school bus or other vehicle owned, leased or used by a school district or school, or through the use of technology or an electronic device owned, leased or used by a school district or school and (ii) at a location, activity, function or program that is not school-related, or **through the use of technology or an electronic device that is not owned, leased or used by a school district or school, if the bullying creates a hostile environment at school for the victim, infringes on the rights of the victim at school or materially and substantially disrupts the education process or the orderly operation of a school**. Nothing contained herein shall require schools to staff any non-school related activities, functions, or programs. The School Committee expects administrators and supervisors to make clear to students and staff that bullying in the school building, on school grounds, on the bus or school-sanctioned transportation, or at school-sponsored functions will not be tolerated and will be grounds for disciplinary action up to and including suspension and expulsion for students, and termination for employees.

b. **Retaliation against a person who reports bullying, provides information during an investigation of bullying, or witnesses or has reliable information about bullying is prohibited.** The District will take appropriate steps to protect from retaliation persons who take action consistent with the bullying plan, or who report, file a complaint of, or cooperate in an investigation of a violation of the bullying plan. Threats or acts of retaliation, whether person-to-person, by electronic means, or through third parties, are serious offenses that will subject the violator to significant disciplinary and other corrective action up to and including expulsion.

c. The Gateway Regional School District will endeavor to maintain a learning and working environment free of bullying.

VI. **DEFINITIONS**

a. "Bullying", the repeated use by one or more school community members of a written, verbal or electronic expression or a physical act or gesture or any combination thereof, directed at a victim that: (i) causes physical or emotional harm to the victim or damage to the victim's property; (ii) places the victim in reasonable fear of harm to himself or of damage to his property; (iii) creates a hostile environment at school for the victim; (iv) infringes on the rights of the victim at school; or (v) materially and substantially disrupts the education process or the orderly operation of a school. For the purposes of this section, bullying shall include cyber-bullying. Bullying is based upon unequal physical, psychological or social power or perceived power. Bullying may occur in a dating relationship. Bullying generally involves a pattern of conduct that is directed at another person, rather than a single, isolated incident. Bullying may include elements of bias (as defined below under Harassment.

b. "Cyber-bullying", bullying through the use of technology or any electronic communication, which shall include, but shall not be limited to, any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system, including, but not limited to, electronic mail, internet communications, instant messages or facsimile communications. Cyber-bullying shall also include (i) the creation of a web page or blog in which the creator assumes the identity of another person or (ii) the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation creates any of the conditions enumerated in clauses (i) to (v), inclusive, of the definition of bullying. Cyber-bullying shall also include the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting creates any of the conditions enumerated in clauses (i) to (v), inclusive, of the definition of bullying.

c. "Cyber-harassment" is defined as any willful and repeated harm inflicted through, but not limited to, Web pages, social networking sites, email, instant messaging or text messaging using computers, cell phones and other electronic devices which is motivated by the target individual or individuals membership in a protected group, whether real or perceived.

d. "Hostile environment" is a situation in which bullying causes the school environment to be permeated with intimidation, ridicule or insult that is sufficiently severe or pervasive to alter the conditions of the student's education. A hostile environment is created and the victim's rights infringed upon creating a disruption of the education process if, following an incident covered in this paragraph, said intimidation, bullying or harassment, by either the perpetrator(s) or anyone acting on their behalf, whether through written, verbal or electronic expression or a physical act or gesture or any combination thereof, continues within the confines of the school building, on school grounds or at a school-sponsored activity, function, program.

e. "Harassment", is defined as unwelcome, intentional, unprovoked discriminatory behavior, toward an individual or individuals, motivated by membership (real or perceived) in a protected category including: race, color, religion, ethinicity/national origin, disability, gender, gender identify, sexual orientation and age. Harassment included cyber-harassment

(see prior definition).

f. "Retaliation" is defined as any form of intimidation, reprisal, or harassment by a school community member directed against another school community member for reporting or filing a complaint, for aiding or encouraging the filing of a report or complaint, for cooperating in an investigation under this plan, or for taking action consistent with this plan.

g. "School Community Member" is defined as any student, district or school employee, school committee member, independent contractor, school volunteer, parent or legal guardian of a student, or a visitor on school premises or at a school-related or school sponsored function or activity.

h. "Sexting" refers to taking, possessing, viewing, sharing, or sending pictures, graphic images, text messages, emails, or other material of a sexually explicit nature on an ECD.

i. "Electronic Communication Devices" (ECDs) may be school-owned or student-owned. Both types may include, but are not limited to, telephones, computers, pagers, cellular telephones, text-messaging devices, personal data assistance device, iPods, iPads, graphing calculators, portable game units or other similar electronic devices.

j. "Material Disruption" can be any of the following:
    i. The necessary cessation of instruction or educational activities.
    ii. An inability of students or educational staff to have access to classroom and out-of-classroom activities.
    iii. The institution of severe or repetitive disciplinary measures in the classroom or during educational and recreational activities to maintain order and protect students, school personnel, and the property of students and school personnel from harm.

k. "Substantial Disruption" means any of the following:
    i. Interference with the ability of students to participate and learn in a safe schooling environment free of intimidation sufficient to cause psychological trauma, physical harm, or threats of physical harm.
    ii. Interference with teaching and administrative responsibilities of school personnel through intimidation sufficient to cause psychological trauma, physical harm, or threats of physical harm.
    iii. Damage, or reasonable fear of damage, to school property or the property of students and school personnel.

VII. SCHOOL'S AUTHORITY OVER SCHOOL-OWNED ECDs ON and OFF CAMPUS

a. Cyber-bullying using school-owned ECDs can begin both on and off campus. Both types have the potential to instantaneously reach a large number of students and public school employees and cause material and substantial disruptions in the schools.

b. Conditions of using school-owned ECDs are set forth in this Policy, violations of which may be subject to disciplinary action by the District.

VIII. SCHOOL'S AUTHORITY OVER STUDENT-OWNED ECDs ON CAMPUS

a. Students have the right to exercise freedom of speech in the classroom and on school grounds. While schools possess broad authority to regulate student-owned ECDs, nothing in this policy

permits school officials to infringe upon students' constitutionally protected right of free speech.

b. The schools may regulate students' possession and use of student-owned ECDs while students are on campus, while attending school-sponsored activities, and while under the supervision and control of school district employees.
c. School personnel possess the discretion to ban ECDs during classroom instruction hours and school-sponsored activities.
d. School personnel may confiscate student-owned ECDs when they have reasonable cause to believe that ECDs have been used to bully or harass other students or employees of the school district, or the use of ECDs will materially and substantially disrupt school activities.
e. School personnel may conduct searches of student-owned ECDs only when they reasonably believe the search will reveal evidence of misuse. The search must not exceed the scope of the alleged misconduct-giving rise to the school official's belief in the necessity of the search.
f. GRSD Policy and Regulations broadly authorizes the school to punish students who use ECDs inappropriately or to bully or harass while attending school or participating in school activities. Students who are on school grounds, going to or coming from school and are on or off campus during school-sponsored activities are considered involved in school activities.

IX. **SCHOOL'S AUTHORITY OVER STUDENT-OWNED ECDs OFF CAMPUS**

a. School Authority is not limited to the geographical boundaries of the school grounds.
b. School officials may regulate students' off-campus use of student-owned ECDs when they can prove there is a strong possibility that the off-campus activity will result in a material disruption of the school environment or a substantial interference with the rights of others.
c. School officials may discipline students for their off-campus use of student-owned ECDs when:
    i. The student knew or should have known that the off-campus ECD communication and/or its effects would appear on campus, meaning that the on-campus consequences were reasonably foreseeable; and
    ii. School officials can demonstrate a causal nexus between the students' off-campus activity and a material disruption of the school environment; or
    iii. Evidence exists that the off-campus communication caused a substantial interference with the rights of others, including the rights of both students and employees to be free from trauma and psychological harm.

X. **UNACCEPTABLE USES**

a. The following uses of the school district system and Internet resources or accounts are considered unacceptable:
    i. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute pornographic, obscene or sexually explicit material.
    ii. Users will not use the school district system to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.
    iii. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate to the educational setting or disruptive to the educational process and

will not post information or materials that could cause damage or danger of disruption.

iv. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

v. Users will not use the school district system to knowingly or recklessly post false or defamatory information about a person or organization, to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

vi. Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.

vii. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district system's security, and will not use the school district system in such a way as to disrupt the use of the system by other users.

viii. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

ix. Users will not use the school district system, or district email, to post private information about another person or to post personal contact information about themselves or other persons including, but not limited to, addresses, telephone

x. numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

xi. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.

xii. Users will not use the school district system to violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

xiii. Users will not use the school district system for the conduct of a business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services, check private email accounts or complete other personal business during the hours that staff is professionally contracted to the district but may use the system, within the guidelines of this AUP, during time that is personal (lunchtime or before/after school).

b. Any use of the system that appears to be inappropriate should be immediately reported to the technology department. If said use is deemed to be inappropriate, the incident will be reported to the building administrator for appropriate discipline. Each building administrator shall maintain a log of all incidents of inappropriate use and log all disciplinary action against the student into the Student Information System.

c. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. A user may also, in certain rare instances, access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher. Examples of such projects may include hate literature, art, or other topics, which would generally be removed by standard filtration software.

XI. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of ECDs, the school district ECD network system and use of the Internet shall be consistent with school district policies and the mission of the school district.

XII. LIMITED EXPECTATION OF PRIVACY

a. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect that the school may at any time, and without prior notice, review the content of personal files on the school district system.
b. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.
c. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time. Inquiries should be made to the network administrator by appointment.
d. School district employees and students should be aware that data and other materials in files maintained on the school district system might be subject to review, disclosure or discovery.
e. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities and activities not in compliance with school district policies conducted through the school district system.

XIII. INTERNET USE AGREEMENT

a. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and employees of the school district.
b. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.
c. The Internet Use Agreement form must be read and signed by the user and the parent or guardian. The form must then be filed at the school office.

XIV. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XV. **USER NOTIFICATION**

a. All users shall be notified of the school district policies relating to Internet use.
    i. This notification shall include the following:
        1. Notification that Internet use is subject to compliance with school district policies.
        2. Disclaimers limiting the school district's liability relative to:
            a. Information stored on school district diskettes, hard drives or servers.
            b. Information retrieved through school district computers, networks or online resources.
            c. Personal property used to access school district computers, networks or online resources.
            d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.
            e. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

b. Notification that, even though the school district may use technical means to limit Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

c. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student or the student's parents.

d. Notification that should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

e. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XVI. **PARENT RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE**

a. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other potentially offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

b. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:
    i. A copy of the user notification form provided to the student user.
    ii. A description of parent/guardian responsibilities.
    iii. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and a supervising teacher prior to use by the student.
    iv. A statement that the school district's acceptable use policy is available for parental review.

XVII. **IMPLEMENTATION; POLICY REVIEW**

a. The school district administration may develop appropriate guidelines and procedures necessary to implement this policy. Such guidelines and procedures shall be an addendum to this policy.

b. The administration shall revise the student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

c. The school district's Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.
d. Because of the rapid changes in the development of the Internet, the school committee shall conduct an annual review of this policy.

Cross References: GRSD Network Responsibility Contract (IJNDB – E)
GRSD Student Use of Electronic Communication Devices (IJNDBB)
GRSD Student Use of Electronic Communication Devices Guidelines & Permission (IJNDBB-E)
GRSD Electronic Communication Devices – Staff Policy, Procedures and Information (IJNDB – E-1)
District Use of District EMail and Social Media File: IJNDD - R