BRADY INDEPENDENT SCHOOL DISTRICT

NETWORK AND INTERNET ACCEPTABLE USE POLICY

I. Introduction

A. Access to the Brady ISD electronic communications system, including the Internet, shall be made available to students and employees exclusively for instructional and administrative purposes in accordance with administrative regulations. The facilities that provide access represent a considerable commitment of District resources for telecommunications, networking, software, etc. This Network and Internet Acceptable Use Policy is designed to help you understand our expectations for the use of those resources in the particular conditions of the Internet and local networks, and to help you use those resources wisely.

B. Usage of the Internet at school is an ‘opt-out’ event for students. Should a parent/guardian wish that their child not participate in Internet activities or usage at school, please send a written notification of the request for nonparticipation to the school principal.

C. Access to the BISD electronic communications system is a privilege, not a right. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with BISD Policies. (See DH, FNC, FNCJ, CQ, and the Student Code of Conduct) Violations of law may result in criminal prosecution as well as disciplinary action by the District. We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in the physical world. To be absolutely clear on this point, all existing District policies apply to your conduct on the Internet and/or local networks, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of District resources, sexual harassment, information and data security, and confidentiality.

D. Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from learning time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the District and expose BISD to significant legal liabilities.

E. The chats, newsgroups, and email of the Internet give each individual Internet user an immense and unprecedented reach to propagate District messages and tell our story. Because of that power we must take special care to maintain the clarity, consistency, and integrity of the District’s educational image and posture. Anything any one student or staff member writes in the course of acting for the District can be taken as representing the District’s educational posture. That is why we expect you to forgo a measure of your individual freedom when you participate in interactive discussions on District time, as outlined below.

F. While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

G. Certain terms in this policy should be understood to include related concepts. District includes our faculty, students, any other employees, and all BISD buildings and equipment, as well as any contracted personnel or equipment. Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including HTML files read in an Internet browser, any file meant to be accessed in a word processing or desktop publishing program, or the files prepared for the Adobe Acrobat reader or other electronic publishing tools. Graphics includes photographs, pictures, animations, movies, or drawings. Display includes monitors, flat panel active or passive matrix displays, LCD's, projectors, televisions, and virtual reality tools. Miscellaneous Devices include IPods, PDAs, MP3 Players, and flash drives.

H. Use of District computing resources implies total acceptance of the terms of the Acceptable Use Policy. The Policy will be printed in the handbooks as well as linked on our web site.

II. Acceptable Use

A. Etiquette

1. The user is expected to abide by the generally accepted rules of network etiquette. The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the district Internet system, including all e-mail, instant messages, Web pages, and Web logs (blogs). These guidelines include, but are not necessarily limited, to the following:
2. Use of electronic mail and other network communications facilities to harass, offend, or annoy other users of the network is forbidden.
3. Do not write or send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or abusive messages to others.
4. Do not post information that could cause damage, danger, or disruption, or engage in personal attacks, including prejudicial or discriminatory attacks.
5. Sexually explicit or suggestive content of any nature is not permissible.
6. Do not reveal personal addresses or phone numbers of students or colleagues.
7. Do not knowingly or recklessly post false or defamatory information about a person or organization.
8. All communications and information accessible via the network should be assumed

to be private property subject to copyright regulations.

9. Do not delete, copy, modify, or examine files and/or data belonging to other users without prior consent.
10. Do not attempt to continue contacting another user after receipt of a request to cease.
11. Do not use District facilities for commercial or political purposes.

B. Management and Administration

1. The District has software and systems in place that can monitor and record all network and Internet usage. We want you to be aware that our security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No user should have any expectation of privacy as to his or her Internet or network usage. Our managers will review Internet and network activity and analyze usage patterns, and they may choose to publicize this data to assure that District Internet and network resources are devoted to maintaining the highest levels of productivity.
2. Attempts to change or evade resource quotas are prohibited.
3. We reserve the right to inspect any and all files, documents, and graphics stored in public or private areas of our networks in order to assure compliance with policy.
4. The display of any kind of sexually explicit image or document on any District system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using our network or computing resources.
5. In compliance with the Children's Internet Protection Act (CIPA), the District uses independently supplied filtering software and data to identify and restrict access to inappropriate or sexually explicit Internet sites. We may block access within our networks to all such sites that we know of. This software works by scanning for objectionable words or concepts, as determined by the District or it's authorized agents. However, no software is foolproof. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had previously been deemed acceptable by any screening or rating program. Please report sites of this nature immediately. If a user sees another user accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.
6. Students and staff may not disable the district's filtering software at any time when students are using the Internet system if such disabling will cease to protect against access to inappropriate materials. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering software has inappropriately blocked access to such sites.
7. The District's Internet and network facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local

jurisdiction in any way. Use of any District resources for illegal activity is grounds for immediate punishment, and we will cooperate with any legitimate law enforcement activity.

8. Any software or files downloaded via the Internet into the District networks become the property of the District. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
9. No user may use District facilities to knowingly download or distribute pirated software or data.
10. No user may use the District's Internet or network facilities to deliberately propagate any virus, worm, Trojan Horse, or trap-door program code.
11. No user may use the District's Internet or network facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy and security of another user.
12. Each user using the Internet and network facilities of the District shall identify himself or herself honestly, accurately, and completely (including one's District affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.
13. Only those users who are duly authorized to speak to the media, to analysts, or in public gatherings on behalf of the District may speak/write the name of the District to any newsgroup, chat room, web log, etc.. Other users may participate in newsgroups or chats in the course of education or business when relevant to their task at hand, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or student of this District, the employee must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the District of any commercial product or service. Only those managers and District officials who are authorized to speak to the media, to analysts, or in public gatherings on behalf of the District may grant such authority to newsgroup or chat room participants.
14. Users are restricted from using District facilities for commercial or political purposes, in any way.
15. Users are reminded that chats, email, web logs, and newsgroups are public forums where it is inappropriate to reveal confidential District information, student data, and any other material covered by existing District secrecy policies and procedures. Users releasing protected information via these methods --- whether or not the release is inadvertent --- will be subject to all penalties in existing data security policies and procedures.
16. Use of District Internet or network access facilities to commit infractions such as misuse of District assets or resources, sexual harassment, unauthorized public speaking, and misappropriation or theft of intellectual property are also prohibited by general District policy, and will be sanctioned under the relevant provisions of the personnel or student handbook.
17. Since a wide variety of materials may be deemed offensive by colleagues, parents,

or students, it is a violation of District policy to store, view, print, or redistribute any document or graphic file that is not directly related to the user's job or education, or authorized activities.

18. Due to bandwidth restrictions, usage of streaming media, Internet radio stations, or information broadcasting services is unacceptable unless for an explicit short term academic use.
19. Users may use their Internet facilities for non-District research or browsing during mealtime or other breaks, or outside of work hours, provided that all other usage policies are adhered to.
20. Users with Internet access may download only software with direct educational or business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.
21. Users with Internet access may not at any time use District Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
22. Users with Internet access may not use District Internet facilities to download images or videos unless there is an explicit District-related use for the material.
23. Users with Internet access may not download any shareware or freeware programs without authorized written consent of an employee of the Information Systems department.
24. Users with Internet access may not upload any software licensed to the District or data owned or licensed by the District without explicit authorization from the manager responsible for the software or data.
25. Staff must supervise student use of the District Internet system in areas under their supervision in a manner that is appropriate to the students' age and circumstances of use.
26. Use of miscellaneous devices is not permitted during school hours, except with the permission and supervision of a teacher. This includes IPods, PDAs, MP3 players, and USB-based 'flash' drives.
27. Non-district owned devices that have wired or wireless Internet or network connectivity (such as laptops, IPods, PDAs, phones, etc) are not permitted on the BISD network except in designated quarantined public access areas due to their inherent security threat.

C. Technical

1. Staff and faculty should attempt to schedule communicationsintensive downloads such as large file transfers, video downloads, mass emailing and the like outside of the instructional day.

D. Security

1. Any file that is downloaded must be scanned for viruses before it is run or accessed.

2. User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet or network resource must keep that password confidential. District policy prohibits the sharing of User IDs or passwords for access to Internet or network sites.
3. The District has installed a variety of firewalls, proxies, and Internet access screening programs and other security systems to assure the safety and security of the District's users and equipment. Any user who attempts to disable, defeat, or circumvent any District security policy will be subject to immediate dismissal.
4. Files containing sensitive District data as defined by existing security policy that is transferred in any way across the Internet must be encrypted.
5. Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connection to any outside computer can be used by an attacker to compromise any District network to which that computer is attached. That is why any computer used for independent dial-up or leased line connections to any outside computer or network must be physically isolated from the District's internal networks.
6. Only those Internet and network services and functions with documented educational or business purposes will be enabled at the Internet firewall.
7. Decryption of system or user passwords is prohibited.
8. Copying or alteration of system files is prohibited.
9. Intentional attempts to "crash" network or Internet systems are prohibited.
10. Any attempts to secure a higher level of privilege on network or Internet systems are prohibited.
11. Vandalism will result in the immediate cancellation of all privileges. Vandalism is defined as any malicious attempt to harm or destroy equipment, data of another user, the BISD networks, or other networks that are connected to the BISD services. This includes, but is not limited to, the uploading or creation of computer viruses.

III. Reliability Clause

A. The Brady ISD offers no warranties of any kind, whether expressed or implied, for the services provided. The Brady ISD will not be responsible for damages suffered, such as loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the District's or user's errors or omissions. Use of any information obtained via the BISD network systems is at the user's own risk. The Brady ISD has no claim for the accuracy or quality of information obtained through network services.

IV. Consequences of Violation

A. Access to the District's electronic communications system is a privilege, not a right. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, CQ series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

B. Students' home and personal Internet use can have an impact on the school and other students. If a students' personal Internet expression – such as a threatening message to another student or a violent Web site – creates a likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.

C. BISD takes bullying and harassment very seriously. Students shall not use any Internet or other communication device to intimidate, bully, harass, or embarrass other students or staff members. Students who engage in such activity on school grounds or who engage in such activity off campus and create a material disruption of school operations shall be subject to penalties for bullying and harassment contained in the student handbook, as well as possible criminal penalties.

D. In the event of a claim that a student has violated this policy, the district will provide the student with notice and an opportunity to be heard in the manner set forth in the student handbook.

V. Exceptions

A. All terms and conditions as stated in this document are applicable to the Brady Independent School District. The terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties. Terms and conditions shall be governed and interpreted in accordance with the laws of the State of Texas and the United States of America. Use of the network or Internet without a signed AUP will be considered implicit and total acceptance of all AUP terms and conditions for access.

BRADY INDEPENDENT SCHOOL DISTRICT

ACKNOWLEDGEMENT OF USER AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATION SYSTEMS AND INFORMATION RESOURCES

User Signature Required Each user authorized to access the district computers, networks, telecommunications, and Internet services is required to sign an acknowledgement form, or signing of the Employee or Student Handbook stating that they have read policy CQ and these rules. As a condition of continued employment, employees, consultants, and contractors must annually sign an acceptable usage policy or Brady ISD Employee or Student Handbook The acknowledgement form will be retained in the employee's personnel file. Agreements from students will be maintained in campus records, as will Agreements from parents.

I hereby acknowledge that I have received information related to the User Agreement for Acceptable Use of the Electronic Communications Systems and Information Resources (commonly known as "Acceptable Usage Policy") as required on Board Policy CQ Legal and CQ Local. I further acknowledge that I have been offered the option to receive a paper copy of said agreement or to electronically access them. I agree to review the Acceptable Usage Policy by accessing the web sites provided or by requesting, in writing, a paper copy from the appropriate department.

An electronic copy can be obtained at http://www.bradyisd.org under Technology Department.

Printed Name____

Campus/Location____

Role: Student, or Employment Position____

User Signature____ Date_______________

Parent/Guardian Signature__________________________________ Date_______________