**STUDENT ACCEPTABLE USE POLICY** **IIBG GUIDELINES**

STUDENT ACCEPTABLE USE OF INFORMATION TECHNOLOGY AND COMMUNICATIONS RESOURCES

The Richfield School District is committed to supporting a safe environment that allows students to learn while using 21st Century skills. Technology resources are provided to enhance and support all teaching and learning. Additionally, the District supports access to information and technology resources by school stakeholders (students, staff, community, parents, etc.) and strives to ensure that the use of technology is efficient, safe, and appropriate.

**Security Measures**

The Internet provides access to a wide range of material. The District expects that staff will blend thoughtful use of the information technology throughout the curriculum.

To the extent possible, the District shall use commercially reasonable technology protection measures that allow it to meet the requirements of the Children's Internet Protection Act, including the use of a filter to protect against access to:

a. Material that is, by definition, obscene (section 1460 of title 18, U.S. Code)
b. Child pornography (section 2256 of title 18, U.S. Code)
c. Material that is harmful to minors (further defined in the Children's Internet Protection Act)

Since no technology protection measure will block 100 percent of the inappropriate material, the District emphasizes the importance of supervision. It is the expectation that all Richfield School District staff will be responsible for monitoring and supervising all users of information technology resources, including the Internet.

Education about online behavior, including interacting on social networking sites and chat rooms, as well as issues surrounding cyber-bullying awareness and response, will be covered in the curriculum each school year.

**Discrimination, Harassment, Cyber-bullying**

All forms of harassment through the use of technology commonly referred to as cyber-bullying, are unacceptable and viewed as a violation of this policy. Cyber-bullying includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings. The District's computer system may not be used to defame others or disclose sensitive personal information about others.

Neither the school's network nor the broader Internet (whether accessed on district property or off, either during school hours or outside school hours) may be used for the purpose of harassment or cyber-bullying. Students' home and personal Internet use can have an impact on the school district and on other students. If students' personal Internet expression, such as a threatening message to a staff member or another student, or a website advocating violence or defamation of another's character, creates a substantial disruption, offenders will be subject to disciplinary and legal actions.

**Internet Safety**

All users are advised that access to the Internet includes the potential for access to materials that are inappropriate or harmful to minors. Staff and students must take responsibility for his or her use of the Internet and avoid sites and activities that are inappropriate or harmful to minors. Staff will provide developmentally appropriate guidance to students as they make use of technology and communication resources. Staff will inform students of their rights and responsibilities as users of the district technology and communication resources.

To the best of its ability, it is the Richfield School District's policy to: (a) prevent access by minors to inappropriate matter on the Internet; (b) instruct in the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) prevent unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) enforce measures restricting minors' access to materials harmful to them per the Children's Internet Protection Act.

**Guidelines for Internet Use**

- All Internet activity is logged and monitored. This information is subject to review at any time.
- Internet access is provided as a supplement to traditional classroom instruction. As such, access to websites with offensive material, adult content, games or non-educational information (music, movie, entertainment, free web hosting sites, etc.) may be blocked
- Any attempts to view adult subject matter, pornography or other offensive materials will result in disciplinary actions
- Students and staff are responsible for any activity that occurs under his/her account
- Students may not reveal personal information about themselves to anyone online who is not a student, staff member, or family member. Students may not post pictures or videos of themselves online without parent approval. Students may not disrupt the learning environment through their use of technology.
- Students should never make appointments to meet people in person that they have contacted on the system without District and parent permission
- Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable

**Use of Social Networking Sites**

The network will block access to, among others, popular social networking sites (MySpace, Facebook, etc.) for the safety of students. Students are also prohibited from using Instant messaging software or services (AOL Instant Messenger, iChat, GoogleTalk, etc.) while using the District network unless directly related to classroom activities and only under the direct supervision of a teacher.

Certain Web 2.0 services (e.g., Discovery Education, Moodle, Voicethreads, wikis, podcasts, RSS feeds, blogs) that emphasize online educational collaboration and sharing among users, may be permitted by

the District; however, such use must be approved by the District. Users must comply with this policy as well as any other relevant policies and rules during such use.

**Website Publishing**

The goals of the Richfield School District website are to provide an effective communication tool between the school district and students, parents, and community; to provide a teaching resource for educators; and to publish student work as a showcase for the achievements of the Richfield School District students. All material posted to the Richfield School District website must follow the guidelines of the above goals, project a positive image of the district, and preserve the confidentiality of students and staff. The following guidelines will be followed:

- All information must accurately reflect the mission, goals, policies, and curriculum of the Richfield School District
- Staff or student work that is published must relate to the curriculum or to a school activity
- Material should be accurate
- Pages must be maintained regularly
- Links to personal home pages is prohibited
- Web pages may not carry advertisements for anything other than school events or school fundraising activities
- No student photographs should be published if the parent/guardian has checked the Opt-out choice on the Student Acceptable Use Policy signature page
- Student first name plus last initial may be used, but never together with a photograph
- Student first name plus last name should not be published
- Content may not reveal home address, phone numbers, other family details, or personal information of staff or students not related to the function within the school district

The district web manager and/or District Administrator may withdraw pages that do not conform to the above guidelines.

**Other Unacceptable Uses**

District resources are to be used for school-related administrative and educational purposes. The user is responsible for his or her actions and activities involving technology. Examples of behaviors **not permitted** while using district information technology and communication resources include, but are **not limited to**:

- Searching for or deliberately viewing, listening to or visiting websites with or known for containing inappropriate material or any material that is not in support of educational objectives, such as profane material, obscene material, sexually explicit material, or pornography
- Attempting to gain unauthorized access to the District system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files, folders or documents without their permission.

- Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies as this may be construed as an unauthorized attempt to gain access, (i.e., computer hacking)
- Attempting to damage or vandalize technology and communication resources
- Using obscene or inappropriate language or content
- Engaging in practices that threaten the network or intentionally waste limited resources (e.g. willfully introducing a virus, downloading music or videos that may overload district server space, gambling, etc.)
- Using District resources for purposes of plagiarism, theft, infringement and other illegal or illicit purposes
- Connecting personal property to District equipment or network, including using personal cellular/mobile technology (e.g., iPhone, Blackberry) devices to access the District's property, networks or Internet access unless directly related to classroom activities and only under the direct supervision of a teacher
- Installing software without permission of the District or using District software in a manner inconsistent with the District's interests, license agreements and applicable laws (violating copyright laws)
- Using District resources to access personal or third party files, information, or electronic mail such as hotmail, yahoomail, gmail, etc.
- Using the system for purposes unrelated to the interests of the District such as use for commercial purposes or personal pleasure or gain
- Attempting to access websites during class time that are not for educational purposes without specific permission from a teacher
- Personal communication via non-District sponsored applications or devices between staff and students, including but not limited to: the use of social networking sites (i.e., Facebook, MySpace), instant messaging and texting
- Engaging in other behaviors in violation of district policy, work rules or law

**Enforcement and Penalties**

Consequences of violations of this Acceptable Use Policy include, but are not limited to, the following actions as deemed appropriate by the District Administrator:

- Suspension of Internet privileges
- Revocation of Internet privileges
- Suspension of network privileges
- Revocation of network privileges
- School suspension
- School expulsion
- Restitution for the cost of the repair and/or technician fees to repair
- Legal action and prosecution by the authorities

We have read and understand the STUDENT ACCEPTABLE USE OF INFORMATION TECHNOLOGY AND COMMUNICATIONS RESOURCES policy and agree to comply with the rules and guidelines.

Student's Name (printed) _____

Student's Name (signature) _____

Grade _____ Teacher _____Date _____

I have read these rules and guidelines and understand that my son/daughter will comply.

Parent's Signature _____

☐ I choose to Opt-out of having my child's photograph/video published on the Richfield School District website. I understand that photos of crowds, audiences and teams may be taken at public events (e.g., assemblies, athletic events, school performances) and may include my child in group pictures. Please do not identify my child's name along with their photograph/video.