BLACK RIVER PUBLIC SCHOOL

# TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

*STUDENT NETWORK AND INTERNET ACCEPTABLE USE, SAFETY & GOOGLE APPS USE*
*2023/2024 SCHOOL YEAR*

Students are encouraged to use Black River computers/network and internet connection for educational purposes. The use of such resources is a privilege, not a right. Students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook, and/or civil or criminal liability. Prior to accessing the network/internet at school, students and parents/guardians must sign in agreement to this Student Network and Internet Acceptable Use and Safety Agreement.

In addition to network access for personal devices and district computers, students will also be issued a Google Apps for Education account in our @brpsk12.org domain.

### *What are Google Apps for Education?*

Black River Public Schools provides staff and students with a Google Apps for Education account. Google Apps is a free web-based suite of programs provided by Google for schools to use. Staff and students in Black River Public Schools have access to Google Apps for Education. Google Apps includes such tools as Google Drive, Google Calendar, and Gmail.

All of the Google Apps services can be accessed from anywhere you have an internet connection (school, home, mobile phone, etc.) This reduces or replaces the need for flash drives and/or external data drives. Since Google Apps is all online, it is the same everywhere you use it. There is no issue with having one version of a program at home and a different version at school. Google Apps allows you to easily share documents and files with teachers and other students, so you can turn in assignments electronically and collaborate on projects with classmates.

If you'd like to know more information about the security of data in Google Apps for Education, please visit http://www.google.com/edu/trust.

### *BR Student Google Account Setup*

Beginning in the fall of 2022, Black River Public School student accounts are created using the student's student number.  This replaces the previous format using the student's last name and first initial. In the event that emails resulted in duplicates, a middle initial or second letter from the first name was added. This is the same for network usernames.  The new student number format eliminates the risk of duplicates as well as simplifying many accounts and services and will gradually replace existing accounts.

### *Uses for Student Gmail*

Email can be a powerful communication tool for students to increase communication and collaboration. Students are expected to check their email multiple times per day. Teachers may send emails to middle and high school students to communicate reminders, course content, pose questions related to class work, or change assignment dates. Students may send email to their teachers with questions or comments regarding class. Students may send emails to other students to collaborate on group projects and assist with school classes.

### *Student Gmail Permissions*

Black River Public Schools' Gmail system controls who email messages can be sent to and who they can be received from. Gmail for students in grades K-3 is limited to communication within the BR domain only.  Students in grades 4-12 may send and receive emails to parents or anyone outside of the district domain. However, the use of student email is subject to monitoring and students should have no expectation of privacy within those emails.

***Student Emails to Staff***

Students are encouraged to email staff concerning school-related content and questions. However, there will be no requirement or expectation for staff to answer student emails outside of their regular work day, although they certainly may if they choose. For example, an unanswered email to a teacher would not excuse a student from turning in an assignment.

***General Email and Online Chat Guidelines***

Below is a general summary of guidelines related to email and any form of online chat or instant messages:
Email and online chat are to be used for school-related communication.

- Do not send harassing email or instant message content. Do not send offensive email or instant message content. Do not knowingly send spam or phishing email or instant messages content.
- Do not send email or instant messages containing a virus or other malicious content.
- Do not send or read email or instant messages at inappropriate times, such as during class instruction.
- Do not send email or instant messages to share test answers or promote cheating in any way.
- Do not use the account of another person.

The smooth operation of Black River's network relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

A. Students are responsible for their behavior and communication on the network/internet. All use of the network/internet must be consistent with the educational mission and goals of the District.

B. Students may only access the network/internet by using their assigned network/internet/Gmail account. Use of another person's account/address/password is prohibited. Students may not allow other users to utilize their passwords. Students are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/devices when leaving them unattended.

C. Students may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the network/internet. Students may not intentionally disable any security features of the network/internet.

D. Students may not use the internet to engage in "hacking" or other unlawful activities.

   1. Students shall not use the network/internet to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a wireless communication device or other electronic equipment is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.

   2. Use of the network/internet to engage in cyberbullying is prohibited. ""Cyberbullying" is defined as the use of information and communication technologies (such as e-mail, cell phone & text messages, instant messaging (IM), defamatory personal websites and/or blogs, and defamatory online personal polling websites); to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (http://www.cyberbullying.ca)]

      Cyberbullying includes, but is not limited to the following:

      a. posting slurs or rumors or other disparaging remarks about a student on a website or on blog;

      b. sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;

      c. using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;

      d. posting misleading or fake photographs of students on websites.

E. Transmission of any material in violation of any State or Federal law or regulation, or school policy is prohibited.

F. Any use of the network/internet for commercial purposes, advertising, or political lobbying is prohibited.

G. Students are expected to abide by the following generally-accepted rules of network/internet etiquette:

    1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the school's computer/network and internet. Do not use obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.
    2. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the internet.
    3. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.
    4. Never agree to get together with someone you "meet" online without prior parental approval.
    5. Check e-mail frequently and delete e-mail promptly from the personal mail directory to avoid excessive use of the electronic mail disk space.
    6. Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). Students should not delete such messages until instructed to do so by a staff member.

H. Use of network/internet to access, process, distribute, display, or print child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the school's computers/network (e.g., viruses) are also prohibited.

I. Malicious use of the network/internet to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited. Students may not engage in vandalism or use the network/internet in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school network, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network/internet security and/or the school's technology protection measures. Students must also avoid intentionally wasting limited resources. Students must immediately notify the teacher, building principal, or the Director of Technology if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access (hacking).

J. All communications and information accessible via the network/internet should be assumed to be private property (i.e. copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.

K. Downloading of information onto the school's hard drives is discouraged; all downloads should be to an external storage device such as a USB drive, a student's Google Drive, or a student's Chromebook. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or software program that infects the network with a virus and causes damage, the student will be liable for any and all repair costs to make the network once again fully operational.

L. Students are prohibited from accessing or participating in online "chat rooms" or other forms of direct electronic communication (other than e-mail) without prior approval from a teacher. All such authorized communications must comply with these guidelines.

M. Privacy in communication over the internet and the network is not guaranteed. To ensure compliance with these guidelines, the school reserves the right to monitor, review, and inspect any directories, files and/or messages residing on or sent using the school's computers/network. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

Users have no right or expectation of privacy when using the network/internet. The District reserves the right to access and inspect any facet of the network/internet, including, but not limited to, computers, devices, network or internet connections, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein.

A student's use of the network/internet constitutes his/her waiver of any right to privacy in anything he or she creates, stores, sends, transmits, uploads, downloads, or receives on or through the network/internet and related storage medium and equipment.

Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to a discovery that a user has violated district policy and/or law. An individual search will be conducted if there is reasonable suspicion that a user has violated district policy and/or law, or if requested by local, State or Federal law enforcement officials. Student's parents have the right to request to see the contents of their children's files, e-mails, and records.

N. Use of the network/internet and any information procured from the network/internet is at the student's own risk. The school is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The school is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from network/internet sources used in student papers, reports, and projects should be cited the same as references to printed materials.

O. Disclosure, use and/or dissemination of personal identification information of minors via the network/internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student network and internet Acceptable Use and Safety Agreement Form."

P. Proprietary rights in the design of websites hosted on the school's servers remain at all times with the school.

Any individual who is aware of a violation of the district policy or this guideline, including inappropriate online contact, content, or conduct, such as sexting, harassment, or cyberbullying, should bring it to the attention of the school principal or Superintendent immediately.