Romoland School District
Responsible Use Policy

Pursuant to:
BP/AR 6163.4 - Student Use of Technology
BP/AR 4040 - Employee Use of Technology

Romoland School District ("District") recognizes that access to technology at school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping our students develop 21st-century technology and communication skills. To facilitate this we provide access to various technologies for student and staff use.

This Responsible Use Policy ("Policy") outlines the guidelines and behaviors that all users are expected to follow when using District technology resources.

- The Romoland School District network is intended solely for educational purposes.
- All activity over the network or using District resources may be monitored and retained.
- Access to online content via the network will be restricted in accordance with our policies and applicable federal regulations, such as the Children's Internet Protection Act ("CIPA").
- Users are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of technology resources may result in disciplinary action.
- Romoland School District makes a reasonable effort to ensure our users' safety and security online but will not be held accountable for any harm or damages that result from the use of District technologies.
- Users of the District network or other technologies are expected to alert Technology staff immediately of any concerns for safety or security.

Technologies Covered: The District may provide technological resources for student and employee use including, but not limited to, Internet access, computers and/or computing devices, videoconferencing capabilities, online collaboration capabilities, message boards, and email. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

Usage Policies: As a condition of maintaining the privilege of using District computer resources, each user will be held responsible for his or her own actions which affect such resources. Each user acknowledges and agrees to abide by the terms of the Policy. A user who violates the Policy will be subject to appropriate discipline.

District technology resources are to be used for instruction, learning, District-related business, and administrative activities. Use of District technology resources to engage in personal business is not permitted.

Internet Access: The District provides its users with access to the Internet, including web sites, resources, content, and online tools. This access will be restricted in compliance with CIPA regulations and District policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users shall comply with the access and security procedures and systems established to ensure the security, integrity and operational functionality of District computer resources.

Users shall not attempt to modify any system or network or attempt to "crash" or "hack" into District systems. Users shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system or security software. Users shall not attempt to remove existing software or add their own personal software to District computers and systems unless authorized.

Personal Safety: Users must never share personal information including phone numbers, addresses, social security numbers, birthdates, or financial information over the Internet or via email. Communicating over the Internet brings anonymity and associated risks and users should always carefully safeguard the personal information of themselves and others. Students should never agree to meet someone they have communicated with online in real life without parental permission.

If you see a message, comment, image, video or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Accounts: Accounts issued to users for the use of District technology resources are for the intended user's sole use only. Users are expected to keep login information private at all times and are responsible for any misuse that occurs under the accounts issued to them. They shall use the system only under their own accounts and shall maintain the privacy of personal information and passwords.

Email: The District may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on District policies.

If users are provided with email accounts they should be used with care. Email is not a secure transmission protocol; messages are sent in clear text and may be intercepted. Users should never send personal information or attempt to open files or follow links from unknown or untrusted origin. Users shall refrain from profanity and vulgarity. Only communicate with other people as allowed by District policies or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Mobile Devices: The District may provide users with mobile computers or other devices to promote learning outside of the classroom. Users are expected to abide by the same responsible use policies when using devices both on and off the District network. Use of these devices while off the District network may be monitored. As a condition of using a District-owned device, the employee or student will be deemed an authorized user of said device and consents to the District's access to the contents of said device as needed by District personnel.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the District is entrusting to your care. Users should report any loss, damage, or malfunction to Technology staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Social/Web 2.0/Collaborative Content: Recognizing the benefits collaboration brings to education, the District may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should never share personally identifying information online.

Cyberbullying: Cyberbullying will not be tolerated. Harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber-stalking are all examples of cyberbullying. Don’t send emails, text messages, or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to cause harm (physically or emotionally) to another person will result in severe disciplinary action. Cyberbullying can be a crime. Remember that your activities are subject to monitoring and retention.

Data Security: District staff and students may have access to confidential and/or personally identifiable information of students or staff. This information may not be shared with unauthorized third parties, and under no circumstances may it be transmitted electronically without the use of appropriate encryption and the prior approval of the Custodian of Records and the Chief Technology Officer. Confidential and/or personally identifiable information may not be stored on mobile computing devices or portable storage devices without encryption, and may not be transmitted via email under any circumstances.

Personal Equipment: The District recognizes that the use of certain technology devices, such as flash drives, which are not owned by the District may be beneficial to both District employees and students. Flash drives and similar storage devices may be used with District computer resources if the user has current security software installed on all non-District equipment on which the flash drive or other storage device is used. District employees and students may connect personal laptops, tablets, or other computing or mobile devices to District wireless networks identified as “Guest” only. Personal equipment may not be connected to any other wired or wireless network owned by the District without express permission by the Chief Technology Officer.

Unless approved by the teacher and/or school administration, students are only permitted to use cellular phones or other mobile communication devices outside of the instructional day (before school, at lunch, and after school). Students must keep their cellular phones or other mobile communication devices powered off and out of sight during instructional time.

As a condition of possessing or using a personally owned device on campus and/or for school related activities, the student will be deemed an authorized user of said device and to have consented to the search of the student's electronic device by a school official when there is a reasonable suspicion that the search will uncover evidence of a violation of the law, Board policy, administrative regulation, or other rules of the district or the school.

District employees may only use personal communication devices during non-duty times of the workday or for brief conversations. Instructional time may not be interrupted by a personal cellular telephone or mobile communication device, except in an emergency. Such activities shall not interfere with the work efficiency or performance of the employee and shall not interfere with the rights or work efficiency or performance of others.

Security: Security on any computer system is of the highest priority. Users who identify a security problem must immediately notify a representative from Technology or an administrator. Users must never use another user’s account or share passwords with anyone, or leave

account/password information where it may be discovered. Students may only use teacher computing equipment under the direct supervision of the teacher, and solely for instructional purposes. Any user identified as a security risk may be denied access to the system.

Downloads: Users shall not download or attempt to download or run executable programs over the District network or onto District resources without express permission from Technology staff.

You may be able to download other file types, such as images or videos. To ensure the security of the network download such files only from reputable sites, and only for educational purposes. Transmission, receiving, or downloading of any material in violation of any U.S. or State regulations is prohibited. This includes, but is not limited to, copyrighted material, pornography, threatening or obscene material or images inappropriate to an instructional environment.

Netiquette: Users are expected to always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users are expected to recognize that among the vast array of valuable content online there also exists unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, future colleges or potential employers to see. Once something is online, it is out there—and can sometimes be shared and spread in ways you never envisioned or intended.

Plagiarism: Users shall not plagiarize content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet must be appropriately cited, giving credit to the original author.

Political Activities: Users shall not use District technology resources for political purposes including, but not limited to, urging the support or defeat of any ballot measure or candidate.

Receipt of Offensive Material: Due to the open and decentralized design of the Internet and networked computer systems, users are warned that they may occasionally receive materials which may be offensive to them. Users should report all such occurrences to the Chief Technology Officer.

No Expectation of Privacy: District technology resources and all user accounts are the property of District. There is no right to privacy in the use of the technology resources or user accounts.

In addition, users are hereby put on notice as to the lack of privacy afforded by electronic data storage and electronic mail in general, and must apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including email, which is transmitted through District technology resources is more analogous to an open postcard than to a letter in a sealed envelope. Under such conditions, the transfer of information which is intended to be confidential should not be sent through District technology resources.

The District reserves the right to monitor and access information contained on its computer resources under various circumstances including, but not limited to, the following circumstances:

Under the California Public Records Act ("CPRA"), electronic files are treated in the same way as paper files. Public documents are subject to inspection through CPRA. In responding to a request for information under the CPRA, District may access and provide such data without the knowledge or consent of the user. If an employee involved in the issue utilized any personal accounts (e.g. personal email, text messaging, social media) to conduct business related to that issue, the employee is required to provide the relevant communications from those personal accounts as part of the district's response to the request.

The District will cooperate with any local, state, or federal officials investigating an alleged crime committed by any person who accesses District computer resources, and may release information to such officials without the knowledge or consent of the user.

The contents of electronic messages, including any email communication sent using District technological resources, may be viewed by Technology staff in the course of routine maintenance, or by the Chief Technology Officer, or designee(s) as needed for District administrative purposes, including, but not limited to, investigation of possible violations of the Policy or other District policies, and monitoring of online activities of minor students.

Examples of Acceptable Use

I will:

- ✓ Use District technologies for instructional activities.
- ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✓ Treat District resources and equipment carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✓ Alert a staff member if I see threatening, inappropriate, or harmful content (images, messages, posts or videos) online.
- ✓ Use District technologies at appropriate times, in approved places, and only for educational pursuits.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that the use of District technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of others and myself.
- ✓ Help to protect the security of District resources.

Examples of Unacceptable Use

I will **not**:

- ✓ Use District technologies in a way that could be harmful.
- ✓ Attempt to find inappropriate images or content, or attempt to circumvent the District's content filtering tools.
- ✓ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✓ Use District technologies to send mass mailings, "spam," or "mail bombs." Mass mailings directed to any large subgroup of District employees or students shall be approved by the sender's immediate supervisor in advance.
- ✓ Plagiarize content I find online.
- ✓ Share personally identifying information, about others or myself.
- ✓ Use District technologies for personal gain, product advertisement, political lobbying, or partisan political activities.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Use District technologies for illegal activities or to pursue information on such activities.
- ✓ Attempt to hack or access sites, servers, or content that is not intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using District technologies.

Limitation of Liability

The District will not be responsible for damage or harm to persons, files, data, or hardware.

While the District employs, and makes reasonable efforts to ensure the proper functioning of filtering and other safety and security mechanisms, it makes no guarantees as to their effectiveness.

The District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the District network.

Violations of this Responsible Use Policy

Student Violations: Users shall report any suspected violation of the Policy by a student to a school site administrator, who shall immediately refer the matter to the Chief Technology Officer for review. If the Chief Technology Officer determines that a violation has occurred, the user may be subject to appropriate discipline, legal action, and/or prosecution.

Employee Violations: Users shall report any suspected violation of the Policy by a District employee to the employee's supervisor who shall immediately refer the matter to the Chief Technology Officer and Director of Human Resources for review. The Chief Technology Officer and/or the Director of Human Resources shall then determine whether a violation of the Policy has occurred. If the Chief Technology Officer determines that a violation has occurred, he or she may take immediate action to restrict, suspend, or revoke the user's privileges. The user may also be subject to appropriate discipline, legal action, and/or prosecution.